

## 1. Didaktische Vorbemerkungen

Die Schülerinnen und Schüler haben in der Regel bereits eine Vorstellung vom Primzahlbegriff. Daher kann man die Begriffe Primzahl und Teiler von den Schülerinnen und Schülern formulieren und präzisieren lassen.

Es stellt sich schnell heraus, dass es schwierig ist, Primzahlen als solche zu erkennen. Vom Sieb des Eratosthenes ausgehend, erleben die Schülerinnen und Schüler über mehrere Stunden hinweg, wie die Methoden, Primzahlen zu erkennen, immer weiter verfeinert werden. Folgt man der vorgelegten Reihenfolge, so kommt man schließlich zu der Aussage, dass eine natürliche Zahl  $n$  eine Primzahl ist, wenn keine der Primzahlen im Intervall  $2 \leq x \leq \sqrt{n}$  ein Teiler von  $n$  ist.

Die nachfolgend dargestellten Beweise sind oft sehr einfach. Es geht natürlich dabei vor allem darum, die Bemerkungen und Sätze möglichst von Schülerinnen und Schülern formulieren und selbst beweisen zu lassen. Da der mathematische Inhalt einfach ist, kann man dabei sein Augenmerk auf die Argumentation und die korrekte mathematische Fachsprache richten.

Einige der anspruchsvolleren Beweise kann man den Schülerinnen und Schülern austeilen und durcharbeiten lassen, damit sie nicht nur selbst mathematische Texte schreiben lernen, sondern auch Erfahrung darin sammeln, selbstständig vorgegebene Texte für sich zu erschließen.

Man kann auch eine Aussage und deren Beweisidee zunächst etwas wage mitteilen und dann die Schülerinnen und Schüler sowohl Aussage als auch Beweis präzisieren lassen. Gut bietet sich hierfür etwa Bemerkung 4 an, besonders, wenn man nicht angibt, unter welchen Voraussetzungen die Bemerkung gilt.

Es folgt am Ende noch der Standardbeweis, dass es unendlich viele Primzahlen gibt, sowie die Weiterentwicklung der Beweisidee, die zeigt, dass es beliebig viele aufeinanderfolgende natürliche Zahlen gibt, die alle keine Primzahlen sind (Primzahlücken).

Um den Text nicht unnötig zu beschweren, ist unter einer „natürlichen Zahl“ im Folgenden stets eine von Null verschiedene natürliche Zahl zu verstehen.

## 2. Begriffe

**Definition 1 (Teiler)** Es seien  $m$  und  $n$  zwei natürliche Zahlen. Ist der Quotient  $m:n$  eine natürliche Zahl, so sagt man, dass  $m$  durch  $n$  teilbar sei. Die Zahl  $n$  heißt in diesem Fall Teiler von  $m$ .

**Definition 2 (Primzahl)** Eine von 1 verschiedene natürliche Zahl, die nur die 1 und sich selbst als Teiler besitzt, heißt Primzahl.

**Alternative Definition** Eine natürliche Zahl, die genau zwei Teiler besitzt, heißt Primzahl.

## 3. Wie erkennt man (kleine) Primzahlen?

Zum Einstieg: Methode des „Sieb des Eratosthenes“ mit der Erstellung einer Primzahlliste bis 200. (vgl. auch elektronische Version des Siebs bei Wikipedia)

**Bemerkung 1:** Ist  $m$  ein Teiler von  $n$ , so ist auch der Quotient  $\frac{n}{m}$  ein Teiler von  $n$ .

**Beweis** Sei  $k = \frac{n}{m}$ . Multipliziert man diese Gleichung mit  $m$  und dividiert man sie mit  $k$ , so bekommt man  $m = \frac{n}{k}$ . Da  $m$  nach Voraussetzung eine natürliche Zahl ist, erweist sich damit  $k$  gemäß Definition 1 ebenfalls als Teiler von  $n$ .

**Bemerkung 2:** Ist  $n$  eine natürliche Zahl, so ist (von  $n$  selbst abgesehen) kein Teiler von  $n$  größer als  $n/2$ .

**Beweis (Widerspruchsbeweis)** Sei  $m$  ein Teiler von  $n$  mit  $m > \frac{n}{2}$  und  $m \neq n$ . Dann folgt aus der Bedingung  $m > \frac{n}{2}$  nach Multiplikation mit 2 die Ungleichung  $2m > n$ . Division durch  $m$  führt zu  $2 > \frac{n}{m}$ . Weil nach Voraussetzung  $m$  ein Teiler von  $n$  ist, muss der Quotient  $\frac{n}{m}$  eine natürliche Zahl sein. Da aber die 1 die einzige natürliche Zahl ist, die kleiner als 2 ist, muss demnach, im Widerspruch zu unserer Annahme  $m = n$  sein.

**Bemerkung 3:** Ist  $m$  ein Teiler von  $n$  und  $k$  ein Teiler von  $m$ , so ist auch  $k$  ein Teiler von  $n$ .

**Beweis** Da  $k$  ein Teiler von  $m$  ist, ist die Zahl  $q$  mit  $q = \frac{m}{k}$  eine natürliche Zahl und es gilt  $qk = m$ . Weil  $m$  ein Teiler von  $n$  ist, ist die Zahl  $p = \frac{n}{m}$  ebenfalls eine natürliche Zahl. Damit haben wir insgesamt:

$$p = \frac{n}{m} = \frac{n}{qk}.$$

Multiplizieren wir die Gleichung mit  $q$ , so erhalten wir

$$pq = \frac{n}{k}.$$

Da  $pq$  als Produkt zweier natürlicher Zahlen selbst eine natürliche Zahl ist, erweist sich somit  $k$  gemäß Definition 1 als Teiler von  $n$ .

**Satz 1:** Ist die natürliche Zahl  $n$  keine Primzahl, so besitzt sie einen von 1 verschiedenen Teiler, der nicht größer als  $\sqrt{n}$  ist.

**Beweis (Widerspruchsbeweis)** Sei  $m$  mit  $m > 1$  ein Teiler von  $n$ , der von  $n$  verschieden ist. Dann ist nach Bemerkung 1 die Zahl  $k$  mit  $k = \frac{n}{m}$  ebenfalls ein Teiler von  $n$ . Da  $m$  verschieden von  $n$  ist, muss  $k > 1$  sein.

Wir behaupten, dass sowohl  $k$  als auch  $m$  größer als  $\sqrt{n}$  sind.

Ist  $m > \sqrt{n}$  und  $k > \sqrt{n}$ , so muss  $m \cdot k > \sqrt{n} \cdot \sqrt{n} = n$  sein, was im Widerspruch zur Definition der Zahl  $k$  steht.

Anmerkung: Wir haben im Beweis eine Rechenregel über Ungleichungen verwendet: Gelten für positive Zahlen  $a, b, c$  und  $d$  die Beziehungen  $a > b$  und  $c > d$ , so kann man daraus auf die Ungleichung  $ac > bd$  schließen. (Bezug zur LPE 3)

Will man also beispielsweise wissen, ob die Zahl 22307 eine Primzahl ist, so genügt es wegen  $\sqrt{22307} \approx 149,35$  alle natürlichen Zahlen zwischen 2 und 149 zu überprüfen. Ist keine davon ein Teiler von 22307, so muss 22307 wegen Satz 1 eine Primzahl sein.

Wie die folgende Überlegung zeigt, kann man sich die Arbeit noch ein wenig erleichtern:

**Satz 2:** Der kleinste von 1 verschiedene Teiler einer natürlichen Zahl  $n$  ist eine Primzahl.

**Beweis (Widerspruchsbeweis)** Ist  $n$  eine Primzahl, so ist sie selbst der kleinste von 1 verschiedene Teiler, der eine Primzahl ist. Daher können wir für den Rest des Beweises annehmen, dass  $n$  keine Primzahl ist.

Ist  $n$  keine Primzahl, so besitzt sie Teiler, die von 1 verschiedenen sind. Sind das alles Primzahlen, so ist eine davon die kleinste und die Behauptung ist bewiesen.

Nehmen wir an,  $n$  besitzt von 1 verschiedene Teiler, und der kleinste davon ist  $p$  und  $p$  ist keine Primzahl. Dann besitzt  $p$  einen von 1 verschiedenen Teiler  $q$ , der nach Bemerkung 2 nicht größer als  $\frac{p}{2}$  ist, der also folglich kleiner als  $p$  ist. Nach Bemerkung 3 ist  $q$  aber auch ein Teiler von  $n$ , was im Widerspruch zur Definition von  $p$  steht.

Um auszuschließen, dass eine Zahl  $n$  eine Primzahl ist, muss man also „nur“ testen, ob die Primzahlen  $x$  im Intervall  $2 \leq x \leq \sqrt{n}$  Teiler von  $n$  sind. Im Fall der Zahl 22307 muss man also nicht alle natürlichen Zahlen zwischen 2 und 149 testen, sondern nur die 35 Primzahlen, die in diesem Intervall liegen.

## 4. Primzahlformeln

Es wäre schön, eine Formel zu haben, mit deren Hilfe man Primzahlen berechnen kann. Genauer: eine Funktion  $f: \mathbb{N} \rightarrow \mathbb{N}$ , die für jede Zahl  $n \in \mathbb{N}$  mit ihrem Funktionswert  $f(n)$  eine Primzahl annimmt. Eine solche Funktion hat man bis heute jedoch nicht gefunden (und man kann vermuten, dass es eine derartige Funktion nicht gibt).

Es gibt jedoch quadratische Ausdrücke, die erstaunliche Ergebnisse liefern. Man kann sie wohl als mathematische Kuriositäten ansehen.

So ist für  $n = 1, 2, \dots, 40$  bei  $f$  mit  $f(x) = x^2 - x + 41$  der Funktionswert eine Primzahl, bei  $g$  mit  $g(x) = x^2 - 79x + 1601$  ist es sogar für  $n = 1, 2, \dots, 79$  der Fall.

Diese Funktionen liefern die Primzahlfolge zwar nicht in der „natürlichen“ Reihenfolge, aber sie erzeugen ihrer einfachen Bauweise zum Trotz doch recht erstaunlich viele Primzahlen.

**Bemerkung 4:** Eine quadratische Funktion  $f$  der Form  $f(x) = ax^2 + bx + c$ ,  $x \in \mathbb{N}$  mit  $a \in \mathbb{Z}^*$ ,  $b, c \in \mathbb{Z}$  und  $|c| \neq 1$  kann nicht ausschließlich Primzahlen als Funktionswerte haben.

**Beweis** Wir nehmen an, dass  $f(n) \in \mathbb{N}$  für alle  $n \in \mathbb{N}$  gilt. Anderenfalls kann die Behauptung 4 gar nicht erfüllt sein. Dann gilt für  $m \in \mathbb{N}$ :

$$f(mc) = a(mc)^2 + bmc + c = c(acm^2 + bm + 1).$$

Da  $a, b, c$  ganze Zahlen sind und  $m \in \mathbb{N}$  gilt, ist  $d$  mit  $d = acm^2 + bm + 1$  eine ganze Zahl. Da  $d$  ein quadratischer Ausdruck in  $m$  ist, kann er für  $m \in \mathbb{N}$  höchstens zweimal den Wert 1 oder 0 annehmen. Man kann  $m$  also so wählen, dass  $d$  von 1 oder 0 verschieden ist. Da  $cd$  dann eine von 0 oder 1 verschiedene natürliche Zahl ist, ist in diesem Fall  $f(mc)$  keine Primzahl, da  $|c|$  und  $|d|$  Teiler von  $f(mc)$  sind.

## 5. Es gibt unendlich viele Primzahlen

**Satz 3:** Es gibt unendlich viele Primzahlen.

**Beweis (Widerspruchsbeweis)** Wir nehmen an, dass es nur endlich viele Primzahlen gibt, etwa  $n$  Stück. Dann muss es eine größte Primzahl geben. Sei  $p_n$  diese Zahl. Jede natürliche Zahl  $m$  mit  $m > p_n$  ist dann keine Primzahl.

Alle Primzahlen lassen sich somit aufzählen:  $p_1, p_2, \dots, p_n$ .

Wir bilden das Produkt  $q$  aller Primzahlen:  $q = p_1 \cdot p_2 \cdot \dots \cdot p_n$ .

Die Zahl  $q$  ist größer als  $p_n$  und somit ist  $q + 1$  erst recht größer als  $p_n$ . Da  $p_n$  die größte aller Primzahlen ist, kann  $q + 1$  keine Primzahl sein. Nach Satz 2 besitzt  $q + 1$  einen Teiler, der eine Primzahl ist, sagen wir  $p_i$ . Dann gilt also

$$\frac{q + 1}{p_i} \in \mathbb{N}.$$

Andererseits haben wir:

$$\frac{q + 1}{p_i} = \frac{p_1 \cdot p_2 \cdot \dots \cdot p_n + 1}{p_i} = \frac{p_1 \cdot p_2 \cdot \dots \cdot p_n}{p_i} + \frac{1}{p_i}.$$

Da in der Aufzählung  $p_1, p_2, \dots, p_n$  alle Primzahlen enthalten sind, ist auch  $p_i$  darin enthalten und der Bruch

$$\frac{p_1 \cdot p_2 \cdot \dots \cdot p_n}{p_i}$$

kann somit durch  $p_i$  gekürzt werden. Daher ist der Bruch eine natürliche Zahl. Da  $\frac{1}{p_i}$  keine natürliche Zahl ist, kann  $\frac{q+1}{p_i}$  als Summe aus einer natürlichen Zahl und einem Stammbruch keine natürliche Zahl sein, was einen Widerspruch darstellt.

## 6. Primzahlücken

Man kann die Argumentation von Satz 3 gewissermaßen umkehren. Es seien  $2, 3, 5, \dots, p$  die ersten  $n$  Primzahlen. Dann ist jede natürliche Zahl  $m$  mit  $m < p$  durch eine dieser Primzahlen teilbar: Entweder ist  $m$  selbst eine dieser Primzahlen oder  $m$  besitzt einen Teiler, der eine Primzahl ist und der damit zu den Zahlen  $2, 3, 5, \dots, p$  gehört. Es sei  $q$  das Produkt der Primzahlen  $2, 3, 5, \dots, p$ . Dann sind die (aufeinander folgenden) natürlichen Zahlen

$$q + 2, q + 3, q + 4, \dots, q + p$$

alle keine Primzahlen, denn  $q$  ist durch jede der Primzahlen  $2, 3, 5, \dots, p$  teilbar und die natürlichen Zahlen  $2, 3, 4, \dots, p$  sind, wie wir uns oben überlegt haben, zumindest durch eine der Primzahlen  $2, 3, 5, \dots, p$  teilbar.

Beispiel: Wir nehmen  $p = 11$ . Dann ist  $q = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$ . Und somit sind die zehn aufeinanderfolgenden Zahlen

$$2310 + 2, 2310 + 3, \dots, 2310 + 11$$

alle keine Primzahlen. Da es unendlich viele Primzahlen gibt, gibt es entsprechend unserer Konstruktion auch Primzahlücken von beliebiger Länge.