Im Folgenden wollen wir uns überlegen, dass es nicht endlich viele Primzahlen geben kann. Dies soll jedoch systematisch und mathematisch korrekt bewiesen werden. Dafür benötigen wir eine gewisse Vorbereitung.

Def. Seien a, b natürliche Zahlen, also $a, b \in \mathbb{N}$. Wir definieren, a *teilt* b, wenn es ein $c \in \mathbb{N}$ mit $a \cdot c = b$ gibt. Kurz schreiben wir dann $a|b$. Teilt a nicht b, schreiben wir auch $a \nmid b$.

Def. Eine natürliche Zahl p heißt *Primzahl*, falls $p \neq 1$ ist und nur von der 1 und sich selbst geteilt wird, also die Aussage $\forall a \in \mathbb{N} : a|p \Rightarrow a = 1 \vee a = p$ wahr ist.

Folgende beiden Lemmata (Hilfssätze) werden uns helfen unser Ziel zu beweisen.

Lemma 1. Seien $a_1, a_2, a_3 \in \mathbb{N}$ mit $a_1|a_2$ und $a_2|a_3$. Dann gilt $a_1|a_3$.

Beweis: Nach der Definition von teilen gibt es natürliche Zahlen c_1 und c_2, so dass $a_1 \cdot c_1 = a_2$ bzw. $a_2 \cdot c_2 = a_3$. Nun ist aber offensichtlich $a_1 \cdot c_1 \cdot c_2 = a_3$. Da $c_1 \cdot c_2 \in \mathbb{N}$ ist, ergibt sich die Behauptung $a_1|a_3$ aus der Definition. □

Lemma 2. Für jede natürliche Zahl $a \neq 1$ gibt es eine Primzahl $p \in \mathbb{N}$ mit $p|a$.

Beweis durch Induktion über a:
Induktionsanfang, $a = 2$: Da 2 eine Primzahl ist und $2|2$, ergibt sich die Behauptung.
Induktionsvoraussetzung: Für jede natürliche Zahl $b \leq a - 1$ mit $b \neq 1$ gibt es eine Primzahl p mit $p|b$.
Induktionsschritt, $a - 1 \mapsto a$: Wir machen eine Fallunterscheidung.
1. Fall, a ist Primzahl: Dann ergibt sich die Behauptung aus $a|a$.
2. Fall, a ist keine Primzahl: Dann muss es aber ein $b \in \mathbb{N}$ geben mit $b|a$, $b \neq 1$ und $b \neq a$ (sonst wäre a eine Primzahl); insbesondere ist $b < a$. Hier greift aber nun die Induktionsvoraussetzung, nach der es eine Primzahl $p \in \mathbb{N}$ gibt die b teilt. Nach dem ersten Lemma ergibt sich $p|a$, also insgesamt die Behauptung. □

Damit haben wir nun die Grundlagen für unser Ziel erarbeitet.

Satz. Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch:
Annahme: Es gibt nur endlich viele Primzahlen; seien $p_1, p_2, ..., p_r$ eine Liste dieser.
Wir betrachten nun die Zahl $c := p_1 \cdot p_2 \cdot ... \cdot p_r + 1$. Nach Lemma 2 gibt es eine Primzahl p die c teilt. Wir können dabei ohne Beschränkung der Allgemeinheit (kurz: o.B.d.A.) sagen, dass $p_1 = p$ ist, da die Reihenfolge in der Liste nicht vorgeschrieben wird. Nachrechnen ergibt aber, dass $(p_1 p_2 ... p_r + 1)/p_1 = p_2 \cdot ... \cdot p_r + \frac{1}{p_1} \notin \mathbb{N}$ ist. Dies ist ein Widerspruch dazu, dass $p_1|c$. Damit ergibt sich, dass die Verneinung unserer Annahme wahr ist. Wir haben unsere Behauptung bewiesen. □

Hoffentlich konnten hier die drei Prinzipen direkter Beweis (vgl. Lemma 1), Beweis durch Induktion (vgl. Lemma 2) und Beweis durch Widerspruch - auch indirekter Beweis genannt - (vgl. Satz) dem Leser näher gebracht werden. Daneben gibt es den Beweis durch Kontraposition: Möchte man die Aussage $\mathcal{A} \Rightarrow \mathcal{B}$ zeigen, dann kann man auch zeigen, dass $\neg\mathcal{B} \Rightarrow \neg\mathcal{A}$ wahr ist, da die beiden Aussagen äquivalent sind.