Satz des Euklid:

Es gibt unendlich viele Primzahlen

29.06.19

Worum es mir hier geht: Meiner Erfahrung nach sind die Mehrzahl aller mathematischen Beweisführungen in den Lehrbüchern dürftig und didaktisch mangelhaft dargestellt. D.h. solche Beweise sind für mich nicht wirklich 100%ig überzeugend. Deshalb ist mein Hauptanliegen in meinen eigenen Beweisdarstellungen, dass ich Beweise möglichst vollständig und somit (gemäß meines Könnens) weitgehend stichhaltig darstelle.

Und eigentlich geht es mir darum, dass man anhand des äußerst instruktiven Beispiels der Beweisführungen in der Mathematik lernt, generell schlüssig und sinnvoll zu argumentieren. Dass man ein Gespür bekommt: was ist überzeugend an einer Argumentation und was nicht.

Satz des Euklid

Der Beweis folgt der YouTube-Vorlesung von Prof. Christian Spannagel vom 15.02.2010: „Die Unendlichkeit der Menge der Primzahlen oder Der Satz des Euklid“. - Spannagel ist einer der ganz Wenigen seiner Zunft, die sich als Mathematiklehrer um die Darstellung lückenloser Beweisführung bemühen, deshalb halte ich mich hier bei diesem Beweis *im sachlichen Kern* an diesen hervorragenden Meister jener Kunst.

Voraussetzungen:

1. **Satz vom kleinsten Teiler:** d teilt n bzw. -> **d**|n
   Der kleinste Teiler **d** $\in \mathbb{N}$
   einer natürlichen Zahl n > 1 ist immer eine Primzahl

***Beweis* (findet sich bei YouTube):** Prof. Christian Spannagel in: Der Hauptsatz der elementaren Zahlentheorie – Teil 1 und Teil 2 (08.12.2010).

Hier jetzt im Einzelnen aufgeführt und ausgefeilt:

Es handelt sich bei den folgenden Ausführungen immer um natürliche Zahlen (geschrieben mit dem Symbol $\mathbb{N}$). Das sind die positiven ganzen Zahlen ab der Zahl 1: $\mathbb{N}$ = 1, 2, 3, 4, 5 usw.

Ein *Teiler* einer natürlichen Zahl geht in dieser Zahl vollständig auf bzw. der Zähler kann ohne Rest durch den Teiler gekürzt werden. Der Teiler steht im Nenner:
z.B. $\frac{100}{50}$. Hier kann 100 von 50 vollständig ohne Rest gekürzt werden zu 2. Geschrieben wird der *Teiler einer Zahl* mit einem senkrechten Strich: 50|100, was bedeutet: „50 ist Teiler der Zahl 100“. Die Zahl 100 hat mehrere Teiler: 2, 4, 5, 10, 20, 25, 50. Alle diese Teiler zusammengefasst bilden die *Teilermenge* der Zahl 100.

Die *Teilermenge* einer bestimmten natürlichen Zahl n sei T(n) genannt – sie ist eine *Teilmenge* der natürlichen Zahlen: T(n) $\subset \mathbb{N}$. Die Eins gehört nicht zu T(n), weil das ja äußerst trivial wäre: denn man kann jede beliebige natürliche Zahl durch 1 teilen, was jeder genaueren Überlegung, wie sie hier angestellt wird, die Tour vermasselt.
T(n) ist definitiv nicht leer, weil zumindest **n** $\in T(n)$ ist, d.h. **n** lässt sich jedenfalls durch sich selbst teilen – wie das ja bei Primzahlen *definitionsgemäß* als einziger Teiler (außer natürlich der 1) der Fall ist.

Nun gibt es nach dem ‚Wohlordnungsprinzip‘ (und nach der einfachen Zahlen-Anschauung) in jeder nicht leeren Teilmenge der natürlichen Zahlen ein kleinstes Element. T(n) hat also ein kleinstes Element. Bezeichnet wird es in diesem Beweis als **d**, **d** $\in T(n)$.

Zu beweisen: d ist eine Primzahl d $\in \mathbb{P}$

Nun kommt **der klassische (sogenannte) *indirekte Beweis***, indem die Alternative als absurd, unhaltbar oder widersprüchlich aufgezeigt wird, womit die Alternative zur Alternative als richtig angesehen wird, sofern es außer diesen beiden Alternativen keine weiteren Möglichkeiten gibt. Die Alternative zu ‚Primzahl‘ ist ‚keine Primzahl‘.

Beispiel aus dem Alltag: Die Wohnungstür hat nur zwei Möglichkeiten, entweder sie ist (mit einem Schlüssel) abgeschlossen oder sie ist nicht abgeschlossen und lässt sich somit normal öffnen. Meine Behauptung, die ich beweisen will, lautet: sie ist abgeschlossen. Nun führe ich die

Alternative zum Widerspruch: ich behaupte stattdessen, sie ist *nicht* abgeschlossen. Und zwar mache ich das, indem ich zur Tür gehe, und versuche sie ohne Schlüssel ganz normal zu öffnen. Das geht aber nicht. Folglich ist die Tür abgeschlossen, was zu beweisen war (w.z.b.w.).

Angenommen **d** $\notin \mathbb{P}$ (**d** wäre *keine* Primzahl; oder mathematisch ausgedrückt: nicht Element der Menge der Primzahlen)

Dann existieren mindestens *zwei* natürliche Zahlen (jeweils >1), a und b als Faktoren, die **d** ergeben: a • b = **d** (und nicht nur lediglich *ein Faktor*, der nur mit 1 multipliziert die Zahl **d** ergibt, wie das bei Primzahlen der Fall ist).
Das bedeutet aber: a|**d** ->(a teilt **d**) oder auch b|**d** **->**(b teilt **d**), denn $\frac{d}{a}$ = b. - D.h. d kann ohne Rest durch a gekürzt werden zur natürlichen Zahl b.

Da ja nach Voraussetzung **d** die kleinste Zahl der Teilermenge T(n) von n ist, gehört **d** also zur *Teilermenge* von n, d.h. es gilt voraussetzungsgemäß **d**|n.

Außerdem ist a<**d** und b<**d**, da die *beiden* Teiler jeweils immer kleiner als die zu teilende nicht-Primzahl sind. (Nur bei Primzahlen gibt es genau eine natürliche Zahl als Teiler, die aber logischerweise genauso groß ist wie die Primzahl).
In a $\cdot b = d$ muss ja die positive ganze Zahl a extra mit einer positiven ganzen Zahl b multipliziert werden, um so groß zu werden wie die positive ganze Zahl **d**. Deshalb ist a<**d.** Wenn ich zur 5 extra noch die Zahl 10 brauche, um 50 zu erreichen, ist klar, dass 5 kleiner ist als 50. Gell?

Wenn also *einerseits* gälte, dass a|n, so ergäbe sich der Widerspruch, dass **d** eben nicht der kleinste Teiler von T(n) ist, da *andererseits* a<**d** ist. Aber wieso ist a auch Teiler von n, wenn a Teiler von **d** ist?

Beispiel: angenommen die kleinste Zahl **d** sei 32 und wir haben zwei Teiler 8 und 4. Und irgendein Vielfaches (etwa das 6-fache) von 32 ergibt die Zahl n. Also n = 6x32 = 192. Nun sind in der Tat 4 und 8 beides Teiler von 192: 192/4=48 und 192/8=24. Da 32 sechs mal in 192 steckt, ergibt sich $n = \frac{192}{4 \bullet 8} = \frac{6 \bullet 32}{4 \bullet 8}$ wo sich also genauso wie in 32 die Zahl 4 oder die Zahl 8 restlos wegkürzen lässt. Also sind 4 oder 8 nicht nur Teiler von **d,** sondern auch von n. Gell?

Prof. Spannagel erklärt das kurz & furz als *Transitivität* der Teilbarkeitsrelation:

a|**d** und **d**|n ⇒ a|n

Da nun die Annahme, dass der kleinste Teiler **d** *keine* Primzahl ist, zum Widerspruch geführt wurde, gibt es für **d** nur noch die Alternative: **d** ist Primzahl!

Nun kommen wir zur zweiten Voraussetzung, die nötig ist für den Beweis vom Satz des Euklid.

2. **Wenn a|b ∧ b|c ⇒ a|(b-c) , wobei b > c ist.** [Auf Deutsch: wenn a Teiler von b ist ***und*** b Teiler von c, dann folgt daraus: a ist Teiler der Differenz (b-c)]

   Beispiel: wenn 50|250 und 50|100 dann gilt: 50|(250-100)

   $\frac{250}{50}$ - $\frac{100}{50}$ = $\frac{250-100}{50}$. Der Punkt ist offenbar der, dass 50 der Nenner des Bruches wird mit dem Zähler 250-100. Und dieser Nenner lässt sich *restlos* bei *beiden* Summanden (genauer: bei Minuend und Subtrahend) im Zähler wegkürzen, ist folglich Teiler jedes der beiden Summanden und folglich auch der Zählersumme (genauer: der Differenz) 250-100. (So ungefähr halt).

Nach diesen beiden Voraussetzungen steht dem vollständigen Beweis des Satzes von Euklid nix mehr im Weg. Auch hier handelt es sich wieder um den klassischen indirekten Beweis, der bei den griechischen Mathematikern des Altertums offenbar zu recht sehr beliebt war.

Annahme (im Gegensatz zur Behauptung) – es gibt *endlich* viele Primzahlen und nicht unendlich viele.
Nach dieser Annahme gibt es also lediglich die endlich vielen k Primzahlen $P_1,P_2,P_3,\ldots,P_k$

Es kann ja nun den Euklid niemand ernsthaft dran hindern, dass er diese k Primzahlen alle miteinander multipliziert und schließlich *Juxes halber* zu diesem Produkt noch eine 1 hinzu zu addiert. Dieses (Produkt+1) sei als **n** bezeichnet:

n= $P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_k + 1$; n ist natürlich auch wieder eine natürliche Zahl: $\boldsymbol{n} \in \mathbb{N}$. Denn alle Primzahlen sind natürliche Zahlen und somit auch deren Produkt und die 1 ist ebenfalls eine natürliche Zahl.

Bekanntermaßen hat jede natürliche Zahl einen kleinsten Teiler, und dieser ist eine Primzahl. (Siehe oben Punkt 1. *Satz vom kleinsten Teiler*).
Sei also p der kleinste Teiler von n: $p \in \mathbb{P}$ mit $p|\mathbf{n}$

Da die Primzahlen gemäß unserer Alternativ-Annahme endlich sind, *muss* dieses p *eine* dieser Zahlen $P_1 \ldots P_k$ sein. Sei P_i diese Primzahl $p=P_i$

Wenn das der Fall ist, so gilt:

erstens $P_i | (P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_k)+1$ (was lediglich eine andere Formulierung von $p|\mathbf{n}$ ist),

zweitens da P_i ja zur Menge aller *endlich* vielen Primzahlen gehört, gehört P_i auch als Faktor zum Produkt dieser Menge = $P_1 \cdots P_k$. Eine Zahl Z von der Größe eines Faktors P_i des Produkts ist dann jedoch Teiler dieses Produkts, weil die Zahl Z ohne Rest gegen P_i gekürzt werden kann. Da $Z=P_i$ ist, so ist P_i Teiler des Produkts $P_1 \cdots P_k$.

M.a.W. es gilt:

$$P_i | (P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_k)+1 \ \wedge \ P_i | (P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_k)$$
$$\Rightarrow P_i | \{(P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_k)+1 - (P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_k)\} \Rightarrow P_i | 1$$

Die Primzahlen fangen jedoch bei 2 an. (Die 1 in $P_i|1$ beispielsweise durch $P_i=2$ geteilt, kann nicht mehr gekürzt werden. Dasselbe gilt logischerweise auch für alle weiteren Primzahlen 3, 5, 7, 11 usw.). ***Deshalb hat Euklid die 1 genommen, denn nur durch die 1 kann die Unhaltbarkeit erzeugt werden***! Das Ergebnis $P_i|1$ ist unhaltbar, und die Annahme *endlich* vieler Primzahlen ist somit falsch. Es kann nur die andere Alternative gelten: es gibt *unendlich* viele Primzahlen.

Die sich hier anschließende Frage ist zweifellos berechtigt: ***wieso ist 1 keine Primzahl?*** Offenbar hat schon Euklid ausgeschlossen, dass 1 eine solche ist. Sonst hätte der Beweis ja nicht geklappt. Später in der Mathematikgeschichte allerdings gab es dennoch diverse Schwankungen ob 1 eine Primzahl ist oder nicht. Mittlerweile ist man übereingekommen, dass das System der Mathematik in sich schlüssiger wird, wenn die 1 keine Primzahl ist. Also hatte Euklid (330-275 v.Chr.) augenscheinlich seinerzeit schon den richtigen Riecher.

Vielleicht gerade auch deswegen, weil der (indirekte) Beweis der Unendlichkeit der Primzahlen so gut funktionierte, wenn die 1 keine Primzahl ist. Somit hätte man hier übrigens ein Anzeichen dafür, dass eine bestimmte Art von *Zirkularität* ein wichtiger Unterbau fundamentalen Denkens darstellen könnte.