19,07,13 –

Hauptsatz der elementaren Zahlentheorie

Jede natürliche Zahl n≥2 besitzt eine eindeutige Primfaktor-Zerlegung (PFZ)

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.

Der Beweis folgt den drei Vorlesungen von Prof. Christian Spannagel vom 2010: Der Hauptsatz der elementaren Zahlentheorie (Teil 1, 2, 3)

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.

Nun zum Verständlichmachen der Aussage dieses Satzes von der Eindeutigkeit der Primfaktorzerlegung (PFZ):

Die Faktoren-Reihenfolge ist nebensächlich – es kommt lediglich auf die tatsächlich gegebenen Zahlen an. Diese sind für jede einzelne natürliche Zahl ≥ 2 fest bestimmt und darum ‚eindeutig'.

Das ist die Behauptung dieses Satzes.

Beispielsweise die Zahl 10 hat folgende Primfaktoren: 2x5

Beispielsweise die Zahl 20 hat folgende Primfaktoren: 2x2x5

Beispielsweise die Zahl 30 hat folgende Primfaktoren: 3x5x2

Die Erfahrung lehrt, dass es für diese Beispielzahlen *genau* diese Primfaktoren gibt. Wie man das ja überhaupt für *alle* kleinen Zahlen unter 100 leicht einsehen kann. Nun ist aber die allgemeine Behauptung: *Jede* natürliche Zahl *n≥2 hat genau nur eine einzige PFZ.*

Beweis:

Voraussetzung für diesen Beweis ist erst mal der ***Satz vom kleinsten Teiler:***

> **Satz vom kleinsten Teiler: d** teilt n bzw. -> **d**|n
> Der kleinste Teiler **d** ∈ ℕ einer natürlichen Zahl n > 1 *ist immer* eine Primzahl

Hier jetzt im Einzelnen der Beweis des Satzes vom kleinsten Teiler aufgeführt und ausgefeilt:

> Es handelt sich bei den folgenden Ausführungen immer um natürliche Zahlen (geschrieben mit dem Symbol ℕ). Das sind die positiven ganzen Zahlen ab der Zahl 1: 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) ⊂ 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** ∈ $T(n)$ 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**, $\mathbf{d} \in T(n)$.

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 $\frac{\boldsymbol{d}}{a}$ = 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 $a \cdot b = \boldsymbol{d}$ 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. Oder?

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

$$n = \frac{192}{4 \cdot 8} = \frac{6 \cdot 32}{4 \cdot 8}$$

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.

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

$$a|\mathbf{d} \text{ und } \mathbf{d}|n \Rightarrow a|n$$

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.

Jetzt zum Beweis des Hauptsatzes:

Prinzipiell geht der so: erst mal muss die ‚***Existenz***' gezeigt werden, dass wenigstens ***eine*** PFZ (Primzahlfaktor-Zerlegung) existiert. Dann wird gezeigt, dass ***nur diese eine*** PFZ existiert.

Sei $n \in \mathbb{N} \setminus \{1\}$ i.W.: Sei n ein Element von $\mathbb{N}$ ohne die Zahl 1. Also: 2,3,4,5,6 usw.

Fallunterscheidung:

Fall 1: $n \in \mathbb{P}$ i.W.: n ist Primzahl (n ist Element der Menge der Primzahlen). Dann hat n tatsächlich einen Faktor, nämlich sich selbst, und der ist in der Tat Primzahl.

Fall 2: $n \notin \mathbb{P}$ d.h. n ist keine Primzahl, hat somit jedenfalls 2 Faktoren $d_1 \cdot q_1 = n$
Formell notiert sieht das folgendermaßen aus:

$$\exists\, d_1, q_1 \in \mathbb{N}\setminus\{1\} \text{ mit } d_1 \cdot q_1 = n$$

Das Zeichen „∃" ist das Existenz-Symbol: „es existiert...". „∈" bedeutet Elementzugehörigkeit: eine Zahl z ist Element von $\mathbb{N}\setminus\{1\}$, also Element der natürlichen Zahlen ohne die 1.

Für den einen Faktor d_1 kann ich mir den kleinsten Teiler nehmen, der ja nach dem Satz vom kleinsten Teiler eine Primzahl ist; und dann bestimme ich noch den zugehörigen Komplementärfaktor

$$q_1 = n / d_1$$

Also etwa im ***Beispiel n=300***: bei 50x6=300 habe ich *nicht* den kleinsten Teiler genommen. Der kleinste Teiler könnte aber 2 sein (einen kleineren gibt es generell nicht, da 1 von der Teilermenge von vornherein ausgeschlossen worden ist). Dann erhalte ich 2x150=300. Der Komplementärfaktor zu d_1=2 ist

$$\frac{300}{2} = 150 = q_1$$

Ich habe also nun schon *eine* Primzahl der PFZ erhalten, nämlich d_1. Um weitere Primzahlen zu erhalten wenden wir die Fallunterscheidung nun auf q_1 an.

Betrachte q_1

Fall 1: $q_1 \in \mathbb{P}$ dann ist die Sache schon erledigt, $d_1 \cdot q_1$ ist die gesuchte PFZ von n
Fall 2: $q_1 \notin \mathbb{P}$ dann wenden wir das Verfahren von oben erneut an: Das heißt es gibt wieder 2 Faktoren $d_2 \cdot q_2 = q_1$ und ich kann für d_2 den kleinsten Teiler nehmen und bestimme anschließend den Komplementärteiler.

Also das obige Beispiel n=300 weiter fortgesetzt. Hier war q_1=150. Wieder bestimme ich den kleinsten Teiler. Da 150 eine gerade Zahl ist, kann ich auch hier wieder die 2 nehmen und der Komplementärfaktor zu $d_2 = 2$ ist $75 = q_2$.

So geht es immer weiter.

Betrachte q_2

Fall 1 Primzahl – dann ok. ***Fall 2*** keine Primzahl dann gibt es wieder zwei Faktoren, von denen ich mir den kleinsten Teiler nehme, denn der ist Primzahl.

Bleiben wir beim obigen Beispiel: wir waren am Punkt q_2 = 75 stehen geblieben. Was könnte hier der kleinste Teiler sein? die 2 kann es nicht sein, aber die Primzahl 3. Also d_3=3 und der Komplementärfaktor q_3=25
Nun kann ich mir wieder 25 vorknöpfen und erkenne: der kleinste Teiler ist d_4=5 und der entsprechende Komplementärfaktor q_4 = 5. Und damit sind wir mit diesem Verfahren am Ende, da d_5=5 eine Primzahl ist. Somit haben wir folgende Primfaktoren:

$$d_1 \cdot d_2 \cdot d_3 \cdot d_4 \cdot d_5 = 2 \bullet 2 \bullet 3 \bullet 5 \bullet 5 = 300$$

Damit ist der erste Teil des Beweises erledigt: Es wurde gezeigt: es existiert in der Tat immer eine gewisse Primfaktorzerlegung für irgendeine natürliche Zahl $n \geq 2$.

Aber ist es auch die einzige PFZ – oder sind (vielleicht bei sehr großen Zahlen n) auch noch andere PFZ möglich?

Das führt dann zum zweiten Teil des Beweises: ***Es gibt genau eine PFZ.***

Hier wird jetzt wieder das klassische Verfahren des indirekten Beweises angewendet.

Allerdings ist der Beweis ziemlich weitläufig und tricky!

Ich nehme also an (im Gegensatz zur Behauptung), es gibt (für einige natürliche Zahlen) *mehr als eine* PFZ und nicht nur eine einzige PFZ. Deshalb würde ich mir diejenigen Zahlen heraus greifen (angenommen, es gäbe sie), die mehr als eine PFZ haben und würde dann diese Menge $M \subset \mathbb{N}\backslash\{1\}$ nennen. ["$\subset$" ist das Symbol für ‚Teilmenge von'. - In diesem Fall: „M ist ***Teilmenge von*** $\mathbb{N}$ außer der 1].

In der Menge M gibt es nach dem Wohlordnungssatz eine kleinste Zahl.
Sei n die kleinste natürliche Zahl mit mehr als einer PFZ.

Hier nun die erste PFZ von n: $n=p_1 \bullet p_2 \bullet p_3 \bullet \bullet \bullet p_k$ mit $p_i , q_j \in \mathbb{P}$

jetzt die zweite PFZ von n: $n=q_1 \bullet q_2 \bullet q_3 \bullet \bullet \bullet q_s$

und folglich $n=p_1 \bullet p_2 \bullet p_3 \bullet \bullet \bullet p_k = q_1 \bullet q_2 \bullet q_3 \bullet \bullet \bullet q_s$

[$p_i \in \mathbb{P}$ bedeutet: *irgendeine* beliebige Zahl aus der Kette der p's ist Element der Primzahlen. Analoges gilt für $q_j \in \mathbb{P}$. – Diese i's und j's aus der Menge $\mathbb{N}$ sind sogenannte ***Indizes (=Mehrzahl von Index)***, die an die allgemeinen Zahlzeichen p, q unten dran gehängt werden.]

Erster Trick:

Die p's und die q's müssen alle paarweise verschieden sein. D.h. es kann kein p_i gleich einem q_j sein.

Denn angenommen es gäbe ein p_i und ein q_j die gleich wären.
Dann wäre $n/p_i = n/q_j = x$

$x= p_1 \bullet p_2 \bullet p_3 \bullet \bullet \bullet p_{i-1} \bullet p_{i+1} \bullet \bullet \bullet p_k = q_1 \bullet q_2 \bullet q_3 \bullet \bullet \bullet q_{j-1} \bullet q_{j+1} \bullet \bullet \bullet q_s$

[Die Zahl p_{i-1} ist der Vorgänger von p_i. Die Zahl p_{i+1} ist der Nachfolger von p_i. Analoges gilt für $q_{j-1} \bullet q_{j+1}$].

Bei den p's fehlt das p_i und bei den q's fehlt das q_j. Da auf beiden Seiten der Gleichung das Gleiche $p_i=q_j$ weggekürzt wurde besteht die Identität. Und es ist klar, dass dann

$n>x= p_1 \bullet p_2 \bullet p_3 \bullet \bullet \bullet p_{i-1} \bullet p_{i+1} \bullet \bullet \bullet p_k = q_1 \bullet q_2 \bullet q_3 \bullet \bullet \bullet q_{j-1} \bullet q_{j+1} \bullet \bullet \bullet q_s$

[Die Zahl x entsteht bei den beiden PFZ's dadurch, dass aus der Kette der p's (=n) das p_i rausgekürzt wurde und aus der Kette der q's (=n) das q_i rausgekürzt wurde. n ist deswegen größer als x, weil in der Kette der positiven Faktoren einer fehlt, nämlich in der einen Kette das p_i, in der anderen das q_i].

Die Annahme ist aber dann echt dumm gelaufen, denn wir hätten hier eine natürliche Zahl x die *zwar* zwei verschiedene PFZ hat, *aber kleiner* als n ist. Im Gegensatz dazu, dass n ja die kleinste Zahl mit verschiedenen PFZ ist. Folglich kann es kein p_i geben, das gleich einem q_j ist.

Da die p's und die q's alle verschieden sind, unterscheidet sich auch p_1 von q_1 und eines von beiden ist logischerweise kleiner.
o.B.d.A. (d.h. *ohne Beschränkung der Allgemeinheit*) kann man davon ausgehen, dass $p_1<q_1$ ist.

Nichts kann einem nun daran hindern, folgende Tricks anzuwenden:

$n/p_1 = p_2 \bullet p_3 \bullet \bullet \bullet p_k = a \qquad \Rightarrow a \bullet p_1 = n$
$n/q_1 = q_2 \bullet q_3 \bullet \bullet \bullet q_s = b \qquad \Rightarrow b \bullet q_1 = n$

Juxes halber bestimmt ***ein mathematischer Schlauberger*** sodann eine Zahl c folgendermaßen:

$$c= n - (p_1 \bullet b)$$

Wenn man b mit q_1 multiplizieren würde, ergäbe das die Zahl n:

$$n/q_1 = b \Rightarrow b \bullet q_1 = n$$

andererseits gilt: $b \bullet p_1 = z$ und wegen $p_1<q_1 \Rightarrow z<n$

[Auch die Sache mit dem $b \bullet p_1 = z$ hat sich der pfiffige mathematische Schlauberger überlegt!].

[Das schöne „⇒" ist das Folgerungs-Zeichen „daraus folgt": „Aus Aussage A folgt Aussage B". Man kann auch sagen: „**wenn** A wahr ist, **dann** ist auch B wahr". Die Sache wird kurz „Implikation" genannt, so dass gleichfalls der Ausdruck „A impliziert B" benutzt werden kann.]

Wenn somit $b \bullet p_1 = z < n$ ist, dann ist $c = (n - z) > 0 \Rightarrow 0 < c$

Aus $c= n - (p_1 \bullet b)$ ergibt sich, wegen $(b \bullet p_1)= z$, $c + z = n$, was bedeutet c braucht noch einen Summanden z , um n zu erreichen. M.a.W.: $c < n$. Folglich gilt die Kette

$$0 < c < n$$

Wegen $a = n/p_1$ ergibt sich $a \bullet p_1 = n$. a braucht also noch einen Faktor um n zu erreichen. Folglich ist $a<n$

Wegen $b = n/q_1$ ergibt sich $b \bullet q_1 = n$. b braucht also noch einen Faktor um n zu erreichen. Folglich ist $b<n$

Jetzt kommt der Salto Mortale:

Da erfahrungsgemäß bekannt ist, dass die ersten natürlichen Zahlen eine eindeutige PFZ haben, können also die Zahlen mit mehrfachen PFZ erst in höheren Zahlbereichen auftauchen. Sodass es also vor diesen Zahlen immer solche mit eindeutiger PFZ gibt.

Und da $a, b, c < n$ ist, die kleinste mit mehrfacher PFZ, so haben a,b,c jeweils genau *eine* eindeutige PFZ.

Nun kommt der Algebraiker zum Zug:

$c= n - p_1 \bullet b = (a \bullet p_1) - (p_1 \bullet b) = p_1 (a - b)$

$c= n - p_1 \bullet b = (b \bullet q_1) - (p_1 \bullet b) = (q_1 - p_1) b$

Somit: $p_1 (a - b) = (q_1 - p_1) b \Rightarrow p_1$ ist ein Teiler der rechten Seite der Gleichung [ebenso wie (a-b), was aber für die folgende Überlegung keine Rolle spielt]:

$$p_1 \mid (q_1 - p_1) b$$

p_1 ist Primzahl, da sie zu einer PFZ von n gehört. Das Produkt $(q_1 - p_1) b$ kann keine Primzahl sein, da eine Primzahl nur einen einzigen Teiler (außer der 1) besitzt und deshalb nicht aus 2 Faktoren bestehen kann, sonst hätte sie zwei Teiler.

Folglich bleibt nur noch übrig, dass p_1 entweder Teiler des einen Faktors oder des anderen Faktors ist.

p_1 teilt aber nicht den Faktor b, weil b aus lauter q's besteht $q_2 \bullet q_3 \bullet \bullet \bullet q_s = b$ und zwar eindeutigerweise, da $b<n$ ist, mit n als die kleinste Zahl mit *mehreren* PFZ. Außerdem sind erwiesenermaßen alle p's unterschiedlich zu den q's – also kann das p_1 sich nicht unter den q's verstecken.

deshalb kann p_1 bestenfalls nur noch den anderen Faktor teilen: $p_1 \mid (q_1 - p_1)$.

Jetzt kommt der letzte faule Trick:

Man sollte folgendes beachten: Es gibt 2 Teilungen. Jedenfalls gilt $p_1 \mid p_1$. D.h. die Primzahl p_1 teilt sich selbst. Des Weiteren sollte jetzt noch gelten $p_1 \mid (q_1 - p_1)$.

Nun gibt es das Gesetz: $s|t \wedge s|u \Rightarrow s|(t+u)$ [das Symbol „∧“ ist das logische „und“, d.i. die logische ‚Konjunktion‘].

Wenn $s|t \wedge s|u \Rightarrow s|(t+u)$ [Auf Deutsch: wenn s Teiler von t ist ***und*** s Teiler von u, dann folgt daraus: s ist Teiler der Summe (t+u)]

> ***Beispiel:*** wenn 50|100 und 50|250 dann gilt: 50|(100+250)
>
> $\frac{100}{50} + \frac{250}{50} = \frac{100+250}{50}$. Der Punkt ist offenbar der, dass 50 der Nenner des Bruches wird mit dem Zähler 100+250. Und dieser Nenner lässt sich *restlos* bei *beiden* Summanden im Zähler wegkürzen, ist folglich Teiler jedes der beiden Summanden und folglich auch der Zählersumme 100+250. (So ungefähr halt).

Es gibt also die beiden Teilungen

$$p_1 \mid p_1 \wedge p_1 \mid (q_1 - p_1) \Rightarrow p_1 \mid [p_1 + (q_1 - p_1)] \Rightarrow p_1 \mid q_1$$

Das geht aber nun mal gar nicht, dass p_1 das q_1 teilt! Es sind beides Primzahlen, die erwiesenermaßen unterschiedlich sind. - Indem wir unser Glück mit irgendeiner solchen Möglichkeit mehrerer PFZ bei einer natürlichen Zahl probierten, haben wir nach langer logischer Odyssee Schiffbruch erlitten und sind beim **Widerspruch** gelandet. Das bedeutet nix anderes, als dass die Annahme, dass es natürliche Zahlen mit mehreren PFZ gibt, schlicht falsch ist. Somit bleibt nur noch übrig, uns damit abzufinden, dass *alle* natürlichen Zahlen ≥ 2 jeweils nur eine einzige PFZ haben.