Primzerlegung in $\mathbb{Z}$

Alexander Hölzle

05.01.2007

Inhaltsverzeichnis

I. Motivation, Überblick und Notation

> Gegenstand der elementaren Zahlentheorie sind in erster Linie die natürlichen Zahlen $1, 2, 3, \ldots$. Nach Kronecker hat sie der liebe Gott geschaffen, nach Dedekind der menschliche Geist. Das ist je nach Weltanschauung ein unlösbarer Widerspruch oder ein und dasselbe. Für die Zahlentheorie ist es gleichgültig, wer die natürlichen Zahlen geschaffen hat. Sie stellt sich auf den Standpunkt, dass sie jedenfalls da sind und uns wohlbekannt sind.

Mit diesen beeindruckenden Worten beginnt H. Hasse seine „Vorlesung über Zahlentheorie“ und identifiziert sogleich den Hauptdarsteller der gesamten Zahlentheorie, die Menge der natürlichen Zahlen $\mathbb{N}$. Allerdings spricht vieles dafür das Studium direkt mit den ganzen Zahlen $\mathbb{Z}$ zu beginnen und den „Umweg“ über die natürlichen Zahlen auszusparen. Interpretiert man also die ganzen Zahlen $\mathbb{Z}$ als Hauptdarsteller, so ist das Hauptthema der Zahlentheorie ohne Zweifel das so genannte **Teilbarkeitsproblem**. Alle Erkenntnisse in diesem Dokument beziehen sich auf die scheinbar so simple Frage

Ist eine ganze Zahl a durch eine andere ganze Zahl b teilbar oder nicht?

Sogar Probleme der höheren Zahlentheorie fußen direkt auf dem Teilbarkeitsproblem oder wurden zumind. dadurch motiviert. Man denke dabei nur an die modernen asymmetrischen Kryptosysteme, wie den RSA-Algorithmus; dessen Sicherheit basiert letztendlich auf dem Teilbarkeitsproblem.

Voraussetzungen zum Verständnis dieses Dokuments benötigt man kaum. Lediglich elementarste Kenntnisse über Gruppen, Ringe und Körper sollten bekannt sein. Wie üblich bezeichnen wir mit $\mathbb{N} := \{1, 2, \ldots\}$ die Menge der natürlichen Zahlen (ohne die 0) und mit $\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ die Menge der ganzen Zahlen. Entsprechend bezeichnen wir mit $\mathbb{N}^0$ die Menge der natürlichen Zahlen inklusive der 0.

II. Prinzip vom kleinsten Element und Induktionsprinzip

In vielen Existenzbeweisen der Mathematik wird entscheidend benutzt das

Prinzip vom kleinsten Element: *Jede nicht leere Menge A von natürlichen Zahlen enthält ein kleinstes Element $a_0 = \min A$.*

Ebenso bedeutend wie das Prinzip vom kleinsten Element ist das

Prinzip der vollständigen Induktion: *Es sei B eine Menge natürlicher Zahlen, so dass folgendes gilt:*

a) Es gibt wenigstens eine Zahl $b_0 \in B$. (Induktionsannahme)

b) Falls $n \in B$, so gilt auch $n + 1 \in B$. (Induktionsschritt)

Aufgrund der Eigenschaften a) und b) enthält dann die Menge B bereits alle natürlichen Zahlen, die größer oder gleich b_0 sind, d.h. es gilt

$$\{x \in \mathbb{N} : x \geq b_0\} \subset B.$$

Beachten Sie, dass sich Induktionsprinzip insbesondere durch die Inklusion auszeichnet!

Im Gegensatz zum Induktionsprinzip ist das Prinzip vom kleinsten Element ob seiner Einfachheit unmittelbar einleuchtend. Umso erstaunlicher ist, dass beide Prinzipien eng miteinander verwandt sind, ja sogar logisch äquivalent. Wir zeigen nun, dass das Prinzip von der vollständigen Induktion eine Konsequenz aus dem Prinzip vom kleinsten Element ist.

Beweis. Es sei B irgendeine Menge mit den Eigenschaften a) und b). Diese Menge B entspricht dem Induktionsprinzip, wenn wir die Inklusion $\{x \in \mathbb{N} : x \geq b_0\} \subset B$ nachweisen. Die geforderte Inklusion $\{x \in \mathbb{N} : x \geq b_0\} \subset B$ besteht genau dann, wenn die Menge

$$A := \{x \in \mathbb{N} : x \geq b_0 \text{ und } x \notin B\}$$

leer ist, d.h. wenn $A = \varnothing$ gilt. Haben wir dies bewiesen, so folgt, dass das die Menge B dem Induktionsprinzip genügt. Der Nachweis dieser Behauptung wird entscheidend mit Hilfe des Prinzips des kleinsten Elements geführt.

Wir nehmen nun an, dass die Menge A nicht leer sei, dann folgt aber mit dem Prinzip vom kleinsten Element, dass die Teilmenge A ein kleinstes Element a_0 beinhalten müsste. Das Element b_0 kann nicht in A liegen, da nach Voraussetzungen a) gilt. Es ergibt sich damit $a_0 > b_0$ und also $n := a_0 - 1 \geq b_0$. Wegen $n < a_0$ gilt $n \notin A$ nach Wahl von a_0. Es folgt: $n \in B$ und aus b) folgt dann aber $a_0 = n + 1 \in B$, d.h. es wäre $a_0 \notin A$ was zum Widerspruch führt. Die Annahme $A \neq \varnothing$ ist also falsch und damit folgt die Behauptung insgesamt. □

Nun deduzieren wir das Prinzip vom kleinsten Element noch aus dem Induktionsprinzip, womit die logische Äquivalenz nachgewiesen sein wird.

Beweis. Es sei $A \subset \mathbb{N}$ irgendeine nicht leere Menge. Wenn $0 \in A$ gilt, so ist 0 ein kleinstes Element. Sei also $0 \notin A$. Wir nennen $b \in \mathbb{N}$ eine (echte) *untere* Schranke von A, wenn für alle $x \in A$ gilt: $x > b$; dabei darf b *nicht* in A liegen, da ansonsten eine echte Ungleichung nicht sicher gestellt wäre. Wir bezeichnen mit B die Menge aller echten unteren Schranken von A, nach Annahme gilt $0 \in B$. Wir wollen beweisen, dass die Menge A kein kleinstes Element besitzt. Dazu nehmen wir an, dass dies nicht gelten würde und leiten mit Hilfe der Menge B einen Widerspruch her:

Vorläufiges Ziel ist es nachzuweisen, dass die Menge B gerade den Aussagen a) und b) des Induktionsprinzips genügt und damit die Inklusion $\{x \in \mathbb{N} : x \geq b_0\} \subset B$ gelten muss. Sei $n \in B$, also $x > n$ für alle $x \in A$. Es folgt $x \geq n + 1$ für alle $x \in A$. Es muss gelten $n + 1 \notin A$, denn sonst wäre $n + 1$ ein kleinstes Element von A (welches nach Annahme nicht existiert). Aus $n + 1 \notin A$ folgt $x > n + 1$ für alle $x \in A$. Dies besagt, dass auch $n + 1$ eine echte untere Schranke von A ist, d.h. $n + 1 \in B$. Damit haben wir für die Menge B die Eigenschaft b) des Induktionsprinzips nachgewiesen. Die Eigenschaft b) folgt wegen $0 \in B$ und damit die Inklusion $\mathbb{N} \subset B$. Dies würde aber $A = \varnothing$ zur Folge haben, da es keine Zahl $a \in \mathbb{N}$ gibt, die größer als jede Zahl $b \in \mathbb{N}$ ist. Widerspruch zur Voraussetzung A nicht leere Menge.

□

Das Induktionsprinzip wird in vielen Varianten benutzt, bspw. könnte man es auch mit Hilfe induktiver Mengen einführen und „beweisen“.

III. Teilbarkeit

Im Ring $\mathbb{Z}$ der ganzen Zahlen sind Addition, Subtraktion und Multiplikation uneingeschränkt ausführbare Rechenoperationen. Für die Division ist dies nicht mehr der Fall, da $\mathbb{Z}$ kein Körper ist. Diese Tatsache ist verantwortlich dafür, dass sich die Zahlentheorie mit $\mathbb{Z}$ beschäftigt bzw. das es überhaupt Zahlentheorie gibt.

1. Ganzzahlige Division

Eine der bedeutendsten Beziehungen, die zwei ganze Zahlen miteinander eingehen können, ist die Teilerbeziehung.

1.1 Definition: Seien a und b ganze Zahlen. Wir sagen, dass die Zahl a die Zahl b **teilt** (oder gleichbedeutend, dass b ein Vielfaches der Zahl a ist), falls es eine ganze Zahl x gibt mit der Eigenschaft

$$b = x \cdot a$$

Das bedeutet, dass bei der Division von b durch a kein Rest über bleibt. Wir notieren diese Eigenschaft kurz mit $a|b$.

Wissen wir also, dass a die Zahl b teilt, also $a|b$, dann muss eine Zahl $x \in \mathbb{Z}$ existieren, so dass $ax = xa = b$ gilt.

1.2 Beispiel: (i) Es gilt $3|6$, $-3|6$, $3|-6$ und $-3|-6$.

(ii) Für jede ganze Zahl a gilt: $a|0$, d.h. $\exists x \in \mathbb{Z}$, so dass $x \cdot 0 = 0$. Offensichtlich ist diese Gleichung für ein beliebiges $x \in \mathbb{Z}$ erfüllt(, da $\mathbb{Z}$ ein Integritätsring ist).

(iii) Für jede ganze Zahl a gilt: $a|a$ mit $x := 1$.

(iv) Die einzigen Teiler der Zahl 1 sind 1 und -1. In der Algebra würde man schreiben: die einzigen Teiler eines Primelements sind die dazu assoziierten.

Ist a ein Teiler von b, so nennt man a auch eine in b **aufgehende Zahl** und b ein **Vielfaches** von a. Zur Beantwortung des Teilbarkeitsproblems kann man mit der multiplikativen Struktur von $\mathbb{Z}$ auskommen; die additive Struktur $(\mathbb{Z}, +)$ wir also nicht notwendig benötigt.

Allerdings kann die Frage, ob a ein Teiler von b ist unter Benutzung der Subtraktion auch wie folgt formuliert werden:

Man entscheide, ob die lineare Gleichung $ax - b = 0$ eine Lösung in $\mathbb{Z}$ besitzt.

Bei dieser Interpretation verschieben wir die Lösungsfindung des Teilbarkeitsproblems in die Theorie einer linearen Gleichung in einer Unbestimmten über $\mathbb{Z}$.Im folgenden Lemma halten wir die grundlegenden Rechenregeln fest:

1.3 Lemma: Seien $a, b, b', c, d \in \mathbb{Z}$. Dann gilt:

(i) $a|b \Rightarrow a|-b$.

(ii) $a|b \Rightarrow a|bc$.

(iii) $a|a$ (Reflexivität)

(iv) $a|b$ und $b|c \Rightarrow a|c$ (Transitivität)

(v) $a|b$ und $a|b' \Rightarrow a|(b+b')$ bzw. $a|(b-b')$.

(vi) $a|b$ und $c|d \Rightarrow ac|bd$.

Beweis. (i) Da $a|b :\Rightarrow \exists x \in \mathbb{Z}$, so dass $ax = b$. Mit $x' := -x$ folgt damit die Behauptung.

(ii) Da $a|b :\Rightarrow \exists x \in \mathbb{Z}$, so dass $ax = b$. Multiplizieren wir diese Gleichung mit c, so erhalten wir $axc = bc$. Es existiert also eine ganze Zahl x', nämlich $x' := xc$, so dass $ax' = bc$ gilt.

(iii) Klar.

(iv) Man wende wieder die Definition an und substituiere.

(v) Aus $a|b$ und da $a|b'$ folgt $\exists x, x' \in \mathbb{Z}$, so dass $ax = b$ bzw. $ax' = b'$. Addieren wir diese Gleichungen, so erhalten wir $ax + ax' = b + b' \Leftrightarrow a(x + x') = b + b'$ und dies zeigt gerade die Behauptung. Analog für $a|(b - b')$.

(vi) Man wende die Definition an und multipliziere die dadurch entstandenen Gleichungen.

□

Man beachte, dass durch die Regel (v) eine Verbindung zwischen Teilbarkeit und Addition hergestellt wird. Ferner könnte man diese Aussage verallgemeinern: Seien $a, b, b' \in \mathbb{Z}$. Aus $a|b$ und $a|b'$ folgt dann $a|(x + b + x'b')$ für alle $x, x' \in \mathbb{Z}$.

Die Regel (iii) ist sofort erweiterbar: Jede ganze Zahl a hat die vier im Allgemeinen verschiedenen Teiler $a, -a, 1, -1$. Diese nennt man die **trivialen Teiler** von a. Alle übrigen Teiler von a heißen **echte Teiler** von a.

1.4 Beispiel:

- Sei a eine natürliche Zahl, die 235 und 252 teilt. Dann ist $a = 1$ oder $a = 17$, denn a muss nach dem letzten Lemma auch die Zahl $252 - 235 = 17$ teilen. Da 17 eine Primzahl ist, muss also $a = 1$ oder $a = 17$ gelten.

- Sei a eine natürliche Zahl, die zwei aufeinanderfolgende Quadratzahlen teilt. Dann ist a ungerade. Denn aus $a|b^2$ und $a|(b+1)^2 \Rightarrow a|(2b+1)$. Also teilt a die Zahl $2b+1$, welche bekanntlich für alle b aus $\mathbb{Z}$ ungerade ist. Da alle Teiler einer ungerade Zahl ungerade sind folgt die Behauptung.

Die Zahl 0 wird von jeder Zahl $a \in \mathbb{Z}$ geteilt, da $0 = a \cdot 0$. Dies ist jedoch auch die einzige Zahl mit unendlich vielen verschiedenen Teilern; dies ergibt sich aus folgender Aussage, die einen wichtigen Zusammenhang zwischen der Teilbarkeitsrelation | und der Anordnungsrelation herstellt.

Wie wir bereits gesehen haben, ist es für die Teilbarkeit unerheblich, ob wir die Zahl a oder $-a$ betrachten. So kennt man bereits alle Teiler der ganzen Zahl a, wenn man alle *positiven* Teiler der natürlichen Zahl $|a|$ kennt. Daher genügt es i.d.R. sich mit der positiven der beiden zu beschäftigen.

1.5 Lemma: Seien $a, b \in \mathbb{Z}$ mit $a|b$. Wenn $b \neq 0$ ist, dann gilt $|a| \leq |b|$. Es gilt sogar entweder $|a| = |b|$ oder $|a| \leq \frac{|b|}{2}$. Insbesondere folgt für positive Zahlen a, b aus $a|b$ auch $a \leq b$.

Beweis. Zunächst seien a und b positive Zahlen aus $\mathbb{Z}$. Da $a|b \Leftrightarrow \exists x \in \mathbb{Z}$, so dass $ax = b$, wobei x ebenfalls positiv sein muss. Ist $x = 1$, so folgt sofort $a = b$ und anderenfalls ist $x \geq 2$. Daraus ergibt sich dann

$$ax = b \Rightarrow a = \frac{b}{x} \leq \frac{b}{2}.$$

Der allgemeine Beweis ergibt sich durch analoge Betrachtungen des Betrages der jeweiligen Zahlen:

Es gilt $b = ax$ mit $x \in \mathbb{Z}$. Hieraus folgt $|b| = |a||x|$. Wegen $b \neq 0$ gilt $a, x \neq 0$, also $|a| \geq 1$ und $|x| \geq 1$. Zusammen folgt $|b| = |a||x| \geq |a|$ und damit ist bereits gezeigt, dass $1 \leq |a| \leq |b|$ gilt. Da es höchstens $2|b|$ verschiedene Zahlen $a \in \mathbb{Z}$ mit $1 \leq |a| \leq |b|$ gibt, welche die Zahl b teilen, hat b höchstens $2|a|$ verschiedene Teiler. □

1.6 Beispiel: Jede ungerade Zahl die 57218 und 57884 teilt ist nicht größer als 333. Wenn a sowohl 57218 als auch 57884 teilt, teilt a auch die Differenz, d.h. $a|666$. Daher ist entweder $a = 666$ oder $a \leq \frac{666}{2} = 333$. Da die Zahl a nach Voraussetzung ungerade ist, kommt $a = 666$ nicht in Frage und damit folgt die Behauptung.

1.7 Folgerung: Seien $a, b \in \mathbb{Z}$ und $-(a-1) \leq b \leq (a-1)$. So gilt:

$$a|b \Rightarrow b = 0.$$

Beweis. Sei b ein Vielfaches von a mit $-(a-1) \leq b \leq a-1 \Leftrightarrow |b| \leq |a-1|$. Angenommen $b \neq 0$, dann folgt mit dem letzten Lemma $|a| \leq |b|$. Dies kann aber nicht sein, da nach Voraussetzungen $|b| \leq |a-1|$ gilt. Widerspruch. □

2. Division mit Rest

Als elementare Anwendung des Prinzips vom kleinsten Element beweisen wir die wohlbekannte Division mit Rest, die bei vielen Beweisen der Mathematik aber insbsondere der Zahlentheorie in $\mathbb{Z}$ eine entscheidende Rolle spielt.

So sichert Satz 1.2.4 nicht nur die Existenz sondern ebenso die Eindeutigkeit der ganzen Zahlen q, r und ist in seiner Bedeutung für die gesamte Mathematik nicht zu unterschätzen.

2.1 Satz: Es seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen und es gelte $b \geq 1$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ zu a, b, so dass gilt:

$$a = qb + r \text{ mit } 0 \leq r < b.$$

Bevor wir diese Aussagen beweisen benennen wir noch die wichtigsten Begriffe in diesem Kontext.

2.2 Definition: Man nennt q den **Quotienten** und r den **Rest bei der Division** von a durch b; im Fall $a \geq 0$ gilt stets $q \geq 0$.

Beweis. Zunächst beweisen wir die **Existenz** der Zahlen q und r. Dazu definieren wir uns die Menge

$$A := \{x \in \mathbb{N} | x = a - zb \text{ mit } z \in \mathbb{Z}\} \subset \mathbb{N}.$$

Dabei ist die Menge A nicht leer, d.h. $A \neq \varnothing$ - dies folgt durch eine einfache Fallunterscheidung: Falls $a \geq 0$, so gilt $a \in A$, schließlich können wir $z := 0$ setzen.
Falls $a < 0$, so gilt $a - ab = a(1-b) \in A$, da $a < 0$ und $1 - b \leq 0$ die Ungleichung $a(1-b) \geq 0$ und damit $a(1-b) \in \mathbb{N}$ zur Folge hat.

Durch Anwendung des Prinzip des kleinsten Elements auf die nicht leere Menge A erhalten wir das kleinste Element von A und bezeichnen es mit r. Da $r \in A$ muss sich r in der Form $r = a - qb \geq 0$ für ein $q \in \mathbb{Z}$ darstellen lassen.

Es gilt notwendig $r < b$, da sonst die Zahl $a - (q+1)b = r - b \geq 0$ ebenfalls nicht negativ aber der minimalen Wahl von r widersprechen würde. Mithin haben wir die gesuchte Gleichung $a = qb + r$ bereits gefunden. Falls $a \geq 0$, so muss $q \geq 0$ gelten, denn $q \leq -1$, d.h. $-q \geq 1$ führt zu $r = a - qb \geq b$.

Nun zeigen wir die **Eindeutigkeit** von q und r:
Es sei neben $a = qb + r, r < |b|$ eine weitere Gleichung $a = q'b + r', r' < |b|$ gegeben, wobei $q', r' \in \mathbb{Z}$ sind. Wir fassen die beiden Gleichungen zusammen

$$\begin{aligned} qb + r = a &= q'b + r' \\ \Rightarrow r - r' &= (q' - q)b \end{aligned}$$

Also gilt die Gleichung $q' - q = \frac{r-r'}{b}$. Wegen $0 \leq r < b$ und $0 \leq r' < b$ gilt $-b < r - r' < b$, also $-1 < \frac{r-r'}{b} < 1$. Da $q - q' \in \mathbb{Z}$, ist also notwendig $q' - q = 0$, d.h. $q' = q$ und damit auch $r' = r$. □

Oftmals interesiert man sich eher für den Rest r als für den Divisor q bei der Division mit Rest. Dies berücksichtigt auch die folgende

2.3 Definition: Seien a und b ganze Zahlen mit $a \neq 0$. Seien q und r die eindeutig bestimmten ganzen Zahlen mit

$$a = qb + r \text{ mit } 0 \leq r < |a|.$$

Dann wird die Zahl r mit $a \mod b$, gesprochen a **modulo** b, bezeichnet.

D.h. $a \mod b$ ist eine ganze Zahl, und zwar die kleinste nichtnegative Zahl r, so dass $a - r$ durch b teilbar ist. Wir können auch schreiben $a = qb + a \mod b$.

2.4 Definition: Seien a und b ganze Zahlen, und sei m eine positive ganze Zahl. Wir schreiben $a = b \mod m$, wenn m die Zahl $(b - a)$ teilt.
Dabei wird $a = b \mod m$ gelesen als „a **ist kongruent zu** b, modulo m“. Die Zahl m wird der **Modulus** genannt. Abkürzend schreiben wir auch anstatt $a = b \mod m$ nur $a \equiv_m b$, wenn die Zahlen a und b kongruent sind.

Die Beziehung zweier ganzer Zahlen $a \equiv_m b$ mit $a, b \in \mathbb{Z}$ erklärt eine Äquivalenz-Relation. Ein Nachweis ist einfach:

- $a \equiv_m a \Leftrightarrow m|(a - a)$, da $m|0$ für jedes $m \in \mathbb{Z}$. Die Relation ist **r**eflexiv.
- Gilt $a \equiv_m b$, d.h. $m|(b - a)$ dann gilt auch offensichtlich $b \equiv_m a \Leftrightarrow m| - (a - b)$. Die Relation ist also **s**ymmetrisch.
- Gilt $a \equiv_m b$ und $b \equiv_m c$, also $m|(b - a)$ und $m|(c - b) \Rightarrow m|((b - a) + (c - b))$. Die Relation ist schließlich auch **t**ransitiv.

Seien $b, b' \in \mathbb{Z}$ zwei ganze Zahlen und $m \in \mathbb{Z}$. Teilen wir nun b, b' durch m, d.h. $b = qm + r$ und $b' = q'm + r'$ mit $0 \leq r, r' < m$, dann gilt $b \equiv_m b'$ genau dann, wenn $r = r'$ gilt.

2.5 Beispiel:

- $8 \mod 3 = 5$.
- $-2 \mod 5 = 3$. Beachten Sie, dass der Rest (gemäß Definition) stets positiv ist.
- Für jede natürliche Zahl a mit $a < m$ gilt $a \mod m = a$.

IV. Primzahlen

Eine elementare und dennoch überaus schwierige Aufgabe der Zahlentheorie besteht darin, eine gegebene Zahl $a > 1$ als ein Produkt von möglichst vielen Faktoren die alle größer als 1 und kleiner als a selbst sind, zu schreiben.

0.6 Beispiel: $1188 = 9 \cdot 11 \cdot 12$ sowie $3315 = 3 \cdot 5 \cdot 13 \cdot 17$ und $512 = 2^9 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$.

Der Vorteil derartiger Faktorisierungen für praktische Berechnungen ist offensichtlich: Mit kleineren Zahlen kann man bequemer rechnen. Zahlen, welche sich nicht weiter zerlegen lassen, wie z.B. 299479 oder 10000079 werden durch folgende Definition herausgehoben.

0.7 Definition: Eine natürliche Zahl $p \in \mathbb{N}$ heißt **Primzahl**, wenn gilt:

a) $p > 1$

b) Ist $p = ab$ mit $a, b \in \mathbb{N}$ eine Produktdarstellung von p, so gilt $a = 1$ oder $b = 1$.

Die Menge aller Primzahlen wird mit $\mathbb{P}$ bezeichnet.

Gemäß dieser Definition ist 1 keine Primzahl, d.h. $1 \notin \mathbb{P}$. Die ersten Primzahlen sind bekanntlich $2, 3, 5, 7, 11, 13, \ldots$.

0.8 Definition: Eine **zusammengesetzte Zahl** n ist eine natürliche Zahl, die sich als Produkt mindestens zweier (gleicher oder verschiedener) Primzahlen darstellen lässt.

Der Begriff der Primzahl lässt sich auch noch anders fassen.

0.9 Lemma: Folgende Aussagen über eine natürliche Zahl $p > 1$ sind äquivalent:

i) $p \in \mathbb{P}$.

ii) 1 und p sind die einzigen positiven Teiler von p.

iii) p hat keine echten Teiler.

Beweis. i) $\Rightarrow$ ii): Gäbe es einen Teiler a von p mit $1 < a < p$, so würde eine Gleichung $p = ab$ mit $b \in \mathbb{N}$ gelten, wo weder $a = 1$ noch $b = 1$ gilt.

ii) $\Rightarrow$ iii): Wäre t ein echter Teiler von p, so auch $|t|$, im Widerspruch zu ii).

iii) $\Rightarrow$ i): Sei $p = ab$ mit $a, b \in \mathbb{N}$. Nach Voraussetzungen hat p nur triviale Teiler , d.h. es gilt entweder $a = 1$ oder $a = p$ und dann $b = 1$. □

Wegen der letzten Eigenschaft iii) nennt man Primzahlen auch häufig *unzerlegbar*. Wir haben die Existenz von Primzahlen durch Probieren sichergestellt. Ohne Probieren ergibt sich das Vorhandensein von Primzahlen aus folgendem

0.10 Satz: (Existenzsatz)
Jede natürliche Zahl $a > 1$ besitzt einen kleinsten (positiven) Teiler $t > 1$; dieser Teiler t ist eine Primzahl.

Beweis. Wir werden zwei Beweise für diese Behauptung angeben. Zunächst ein Induktionsbeweis nach a:

Für $a = 2$ ist die Behauptung richtig, denn 2 ist eine Primzahl und natürlich gilt $2|2$. Es gilt also der Induktionsanfang. Wir nehmen nun $a > 2$ an und es gelte die Induktionsvoraussetzung für alle natürlichen Zahlen kleiner als a.

Ist a selbst prim, d.h. $a \in \mathbb{P}$, so ist die Behauptung offensichtlich wahr. Sei nun a nicht prim, also zusammengesetzt. Gemäß Definition existiert also eine Zahl $t \in \mathbb{N}$ mit $1 < t < a$ und $t|a$. Nach Induktionsvoraussetzung hat t selbst einen Primteiler, welcher dann auch Primteiler von a ist.

Nun der zweite klassische Widerspruchs-Beweis:

Die Menge T aller positiven Teiler $\neq 1$ von a ist nicht leer, da $a \in T$. Nach dem Prinzip vom kleinsten Element enthält T ein kleinstes Element t. Diese Zahl ist der kleinste positive Teiler > 1 von a. Wäre t nicht Primzahl, so gäbe es einen Teiler t' von t mit $1 < t' < t$. Aus $t'|t$ und $t|a$ folgt wegen der Transitivität der Teilbarkeit, dass t' ein Teiler von a wäre. Wegen $t' > 1$ würde t' also zur Menge T gehören. Wegen $t' < t$ ist das ein Widerspruch zur minimalen Wahl von t. □

Bereits EUKLID bewies vor über zweitausend Jahren, dass es unendlich viele Primzahlen geben muss. Allerdings versuchte *Euklid* den Begriff der Unendlichkeit zu vermeiden:

Die Primzahlen sind mehr als jede vorgegebene Menge von Primzahlen.

Die Beweisführung von *Euklid* ist ungemein scharfsinnig und ruft Bewunderung bei den meisten Mathematiker hervor. Dabei beweist *Euklid* mehr als eigentlich gefordert: Der Beweis liefert ein Verfahren, immer neue Primzahlen zu konstruieren. Wir werden also zeigen:

0.11 Satz: Es gibt unendlich viele Primzahlen.

Wobei wir den folgenden Satz beweisen werden.

0.12 Satz: (Satz von Euklid)
Es seien $p_1, p_2, \ldots, p_n$ endlich viele Primzahlen (die irgendwie vorgegeben sind). Dann ist der kleinste (positive) Teiler $t > 1$ der natürlichen Zahl

$$a := p_1 p_2 \cdot \ldots \cdot p_n + 1$$

eine Primzahl, die von allen Primzahlen $p_1, p_2, \ldots, p_n$ verschieden ist.

Es dürfte klar sein, dass die Unendlichkeit der Menge $\mathbb{P}$ aus dem Beweis des Satzes von Euklid als Spezialfall folgt.

Beweis. Da $a > 1$, existiert t, und zwar ist t gemäß dem Existenzsatz eine Primzahl. Würde t mit einer der Zahlen $p_1, p_2, \ldots, p_n$ übereinstimmen, so wäre t damit auch Teiler des Produkts $p_1 p_2 \ldots p_n$. Aus $t|a$ und $t|(p_1 p_2 \ldots p_n)$ und $1 = a - p_1 p_2 \ldots p_n$ folgt $t|1$ aus den Rechenregeln (Lemma 2.1.1). Da aber 1 nur die Teiler 1 bzw. -1 hat, wäre $t = 1$ im Widerspruch zu $t > 1$, da t gemäß Existenzsatz prim ist. □

Die natürlichen Zahlen wachsen wohlbekannt ins Unendliche und zu jeder Zahl $n \geq 2$ existiert ein Primteiler, diese beiden Tatsachen erzwingen damit die Unendlichkeit der Menge $\mathbb{P}$.

Führen wir das beschriebene Konstruktionsverfahren sukzessive durch, so erhalten wir eine Reihe von natürlichen Zahlen, die nicht unbedingt prim sein müssen. Ausgehend von $n = 1$ und der kleinsten Primzahl 2 erhalten wir: $a_1 := 2$ im ersten Schritt und $a_2 := 2 + 1 = 3$ und damit für t die zweitkleinste Primzahl 3. Weiterhin erhalten wir $a_3 := 2 \cdot 3 + 1 = 7$ sowie $a_4 := 2 \cdot 3 \cdot 7 + 1 = 43$ sowie $a_4 := 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807 = 13 \cdot 139$. Wie wir sehen ist a_4 keine Primzahl. Bestimmt man die kleinsten Teiler der jeweiligen Glieder der Folge a_n, so erhält man eine nicht monoton steigende Folge von Primzahlen.

Auch in der Kryptographie bzw. in der theoretischen Informatik benötigt man oftmals folgende Abschätzung.

0.13 Lemma: Ist a eine zusammengesetzte Zahl, dann existiert ein Primteiler p von a mit $p \leq \sqrt{a}$.

Beweis. Ist a zusammengesetzt, dann ist der kleinste Teiler p von a eine Primzahl (Existenzsatz). Es gilt dann also $p \leq \frac{a}{p}$, also $p^2 \leq a$. □

Möchte man also nachweisen, ob eine natürliche Zahl a eine Primzahl ist oder nicht, so muss man nur feststellen, ob sie durch eine Primzahl $\leq \sqrt{a}$ teilbar ist oder nicht.

0.14 Beispiel: 257 ist prim, da $2 \nmid 257, 3 \nmid 257, 5 \nmid 257, 7 \nmid 257, 11 \nmid 257, 13 \nmid 257$. Die nächste Primzahl 17 ist größer als $\sqrt{257}$.

0.15 Lemma: (Fundamentallemma)
Teilt eine Primzahl p ein Produkt positver natürlicher Zahlen ab, so teilt p genau einen der beiden Faktoren.

Beweis. Die Menge $E := \{x \in \mathbb{N} : p|ax\}$ enthält p und b, da nach Voraussetzung $p|ab$. Nach dem Prinzip vom kleinsten Element existiert also ein Minimum $c \in \mathbb{N}$ der Menge E. Beweisentscheidend ist nun die Behauptung, dass das Minimum c aus E jedes weitere Element y aus E teilt, d.h. es soll gelten $c|y$ für jedes $y \in E$:
Nach dem Satz von der Division mit Rest gilt eine Gleichung $y = qc + r$ mit $q, r \in \mathbb{N}^0$, $0 \leq r < c$. Aus $y \in E$ bzw. $c \in E$ und

$$\begin{aligned} & y = qc + r \\ \Rightarrow\ & r = y - qc \\ \Rightarrow\ & ar = ay - q(ac) \end{aligned}$$

folgt, dass $p|ar$; schließlich teilt p die Zahlen ay und ac.
Wäre $r > 0$, so läge r in E, was wegen der Minimalität von c und $r < c$ nicht sein kann. Es muss also $r = 0$ gelten, d.h. $c|y$. Damit haben wir die Teilbehauptung bewiesen.

Setzen wir $y := p$, so folgt $c|p$. Wegen Lemma 3.1 sind daher nur zwei Fälle möglich: $c = 1$ oder $c = p$. Im Falle $c = 1$ gilt $p|a$ wegen $p|ac$. Im Falle $c = p$ folgt $p|b$ wegen $b \in E$. □

Es sei angemerkt, dass obiger Beweis wesentlich einfacher und eleganter mit algebraischen Methoden (Idealen) geführt werden kann. Da dieses Dokument jedoch eine elementare Einführung ist, haben wir darauf verzichtet.

Man beachte, dass die Aussage des Fundamentallemmas rein multiplikativ ist, während in seinem Beweis auch die additive Struktur von $\mathbb{N}$ eingeht, und zwar in entscheidender Weise. Eine Verallgemeinerung des letzten Lemmas folgt mit vollständiger Induktion.

0.16 Folgerung: Teilt eine Primzahl p ein Produkt $a_1 \cdot \ldots \cdot a_n$ aus n positiven natürlichen Zahlen $a_1, \ldots, a_n$, so teilt p einen der Faktoren.

Beweis. (Induktion nach n)
Die Fälle $n = 0$ und $n = 1$ sind trivial. Sei die Behauptung richtig für Produkte von $n-1$ positiven natürlichen Zahlen. Teilt dann p das Produkt $(a_1 \cdot \ldots \cdot a_{n-1}) \cdot a_n$ der n natürlichen positiven Zahlen, so folgt aus dem Fundamentallemma, dass entweder $(a_1 \cdot \ldots \cdot a_{n-1})$ oder a_n durch p geteilt wird. Im ersten Fall erhält man aus der Induktionsvoraussetzung, dass p eine der Zahlen $a_1, \ldots, a_{n-1}$ teilt, so dass stets einer der Faktoren $a_1, \ldots, a_n$ von p geteilt wird. □

Das Fundamentallemma ermöglicht eine neue und wichtige Charakterisierung der Primzahlen, die nicht mehr auf der „Unzerlegbarkeitseigenschaft“ dieser Zahlen basiert und die im Folgenden eine bedeutende Rolle spielen wird.

0.17 Satz: Folgende Aussagen über eine natürliche Zahl $p > 1$ sind äquivalent:

i) p ist eine Primzahl.

ii) Aus $p|(ab)$ mit $a, b \in \mathbb{Z}$, folgt $p|a$ oder $p|b$.

Beweis. i) ⇒ ii): Falls $a = 0$ oder $b = 0$, so ist nichts zu zeigen. Sonst kann man durch Übergang zum Negativen ohne Einschränkung a und b als positiv annehmen und hat

somit die Voraussetzungen des Fundamentallemmas erfüllt.

ii) $\Rightarrow$ i): Sei t irgendein positiver Teiler von p. Dann gilt eine Gleichung $p = tt'$ mit $t' \in \mathbb{N}$. Dies bedeutet $p|tt'$. Nach Voraussetzungen folgt $p|t$ oder $p|t'$. Da $1 \leq t, t' \leq p$ folgt $t = p$ oder $t' = p$, d.h. $t = p$ oder $t = 1$. Mithin hat p nur die positiven Teiler 1 und p, ist also nach dem Lemma 3.1 eine Primzahl. □

Die Eigenschaft ii) des Satzes nennt man (im Unterschied zur Unzerlegbarkeitseigenschaft) *Primeigenschaft*. Wir können den Satz also so formulieren:

> *Eine natürliche Zahl $p > 1$ ist genau dann unzerlegbar, wenn sie die Primeigenschaft besitzt.*

V. Hauptsatz der elementaren Zahlentheorie

In diesem Abschnitt werden wir den Hauptsatz der elementaren Zahlentheorie beweisen. Dazu präzisieren wir zunächst die durch Probieren gewonnene Einsicht, dass man jede natürliche Zahl so lange Faktorisieren kann, bis man bei lauter unzerlegbaren Faktoren, bei „Primfaktoren“, angelangt ist.

Der Weg auf dem man solche „Primzerlegungen“ herstellt, ist nicht kanonisch, so kann man z.B. für die Zahl 60 wie folgt vorgehen:

$$60 = 6 \cdot 10 = 2 \cdot 3 \cdot 2 \cdot 5 \quad \text{oder} \quad 60 = 4 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5. \tag{V.1}$$

Die Primzahlen, die in einer solchen endlichen Produkt-Darstellung einer natürlichen Zahl $a \in \mathbb{N}$ auftreten, heißen **Primfaktoren** der Zahl a. Die Produktdarstellung selbst heißt **Primzerlegung** bzw. **Primfaktorzerlegung**. Es erweist sich als zweckmäßig, auch Produkte mit null Faktoren zuzulassen (leere Produkte). Dazu treffen wir folgende formale

Konvention:
Ein Produkt $p_1 p_2 \cdot \ldots \cdot p_n$ aus n Faktoren hat im Spezialfall $n = 0$ den Wert 1.

Diese Konvention mag zunächst verwundern, ist aber in Analogie zur Verabredung bei Summen zu verstehen, wo man unter einer Summe $c_1 + \ldots + c_n$ von n Summen im Spezialfall $n = 0$ üblicherweise den Wert 0 versteht (leere Summe). Gemäß unserer Konvention besitzt auch die Zahl 1 eine Primzerlegung mit 0 Primfaktoren.

In beiden Fällen ergibt sich in (4.1) bis auf die (willkürliche) Reihenfolge der Primfaktoren *dieselbe* Zerlegung und wir werden zeigen, dass dies kein Zufall ist. Zunächst zeigen wir jedoch die

0.18 Satz: (Existenz einer Primzerlegung)
Jede natürliche Zahl $a \geq 1$ besitzt eine Primfaktorzerlegung

$$a = p_1 \cdot p_2 \cdot \ldots p_n.$$

Dabei kann man für p_1 speziell den kleinsten Primteiler t von a wählen.

Beweis. Wir führen den Beweis mit Induktion nach a. Für $a := 1$ trifft die Behauptung zu (leeres Produkt), ebenso für $a := 2$, denn 2 ist prim. Es gilt also die Induktionsverankerung.

Sei $a > 1$, und sei vorausgesetzt, dass die Behauptung für alle natürlichen Zahlen a' mit $1 \leq a' < a$ richtig ist. Nach dem Existenzsatz (vgl. Abschnitt IV) besitzt a einen kleinsten Primteiler t. Es besteht dann eine Gleichung

$$a = tb \qquad \text{mit } 1 \leq b < a \text{ (wegen } 1 < t \leq a).$$

Nach Induktionsvoraussetzung hat b eine Primzerlegung

$$b = p_2 \cdot \ldots \cdot p_n.$$

Setzt man $p_1 := t$, so ergibt sich für a folgende Primzerlegung

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_n.$$

□

Sei $a \in \mathbb{N}$ vorgegeben. Soll nun die Primfaktorzerlegung bestimmt werden, so ist die Schul-Methode meist die praktikabelste, zumind. bei hinreichend kleinen Zahlen a.

0.19 Beispiel: Wir bestimmen die Primfaktorzerlegung von 30. Dazu versuchen wir nacheinander in aufsteigender Reihenfolge, ob eine Primzahl p die vorgegebene Zahl 30 teilt. D.h. wir prüfen, ob 2 die Zahl 30 teilt, was offensichtlich zutrifft. Sodann überprüfen wir, ob 2 die Zahl 15 teilt, was nicht der Fall ist. Nun überprüfen wir, ob die nächst größere Primzahl 3 die 15 teilt. Dieses Vorgehen führen wir iterativ fort und erhalten dadurch die Primfaktorzerlegung $30 = 2 \cdot 3 \cdot 5$.

Wieder Euklid bewies um 300 v.Chr. die Eindeutigkeit der Zerlegung einer natürlichen Zahl in Primzahlfaktoren. Es sei konstatiert, dass die logische Selbstverständlichkeit der Eindeutigkeit der Primfaktorzerlegung ein Irrglaube ist. Meist erst bei sehr großen Zahlen verliert sich meist dieses Verurteil im Zweifel. Umso erstaunlicher ist es, dass Euklid die Notwendigkeit verspürte diesen Beweis zu führen.

0.20 Satz: (Eindeutigkeit der Primzerlegung)
Die Primzerlegung einer jeden natürlichen Zahl $a \geq 1$ ist bis auf die Reihenfolge der Primfaktoren eindeutig.
Genauer: Sind $a = p_1 \cdot \ldots \cdot p_n$ und $a = q_1 \cdot \ldots \cdot q_m$ zwei Primzerlegungen von a mit Primzahlen $p_1, \ldots, p_n, q_1, \ldots, q_m$, so gilt $m = n$, und man kann die Primzahlen der zweiten Zerlegung so (um)numerieren, dass gilt $p_1 = q_1, \ldots, p_n = q_n$.

Beweis. Wir führen wieder Induktion, diesmal nach der Anzahl der Primfaktoren n. Für $n = 0$ ist $a = 1$ und damit notwendigerweise auch $m = 0$. Es gilt also die Induktionsverankerung.

Sei die Behauptung nun für alle positiven natürlichen Zahlen bewiesen, die eine Primzahlzerlegung mit $n - 1$ Primfaktoren zulassen, wobei $n \geq 1$ (Induktionsvoraussetzung). Sind $a = p_1 \cdot \ldots \cdot p_n$ und $a = q_1 \cdot \ldots \cdot q_m$ zwei Primzerlegungen von a, so besagt die Gleichung $p_1 \cdot \ldots \cdot p_n = a = q_1 \cdot \ldots \cdot q_m$ speziell $p_1 | (q_1 \cdot \ldots \cdot q_m)$. Gemäß Folgerung 3.7 folgt daraus $p_1 | q_j$

für einen Index j mit $1 \leq j \leq m$, wobei man nach Umnumerieren von $q_1, \ldots, q_n$ o.B.d.A. $j = 1$ annehmen darf. Da q_1 eine Primzahl ist, ergibt sich wegen Lemma 3.1 und $p_1 > 1$ die Identität $p_1 = q_1$. Aufgrund der Kürzungsregel besitzt die Zahl $a' := p_2, \ldots, p_n$ also noch die weitere Primzerlegung $a' := q_2, \ldots, q_m$, wobei erstere aus $n-1$ Primfaktoren besteht. Nach der Induktionsvoraussetzung folgt dann $n-1 = m-1$ und, nach geeignetem Umnumerieren, $p_2 = q_2, \ldots, p_n = q_n$. Somit ist die Eindeutigkeit der Primfaktorzerlegung bewiesen. □

Bemerkung: Der soeben geführte *Eindeutigkeitsbeweis* benutzt versteckt (beim Verwenden der Division mit Rest im Beweis des Fundamentallemmas), aber entscheidend die additive Struktur von $\mathbb{N}$. Im Beweis der *Existenz* einer Primzerlegung wird die additive Struktur von $\mathbb{N}$ nicht herangezogen. Da Primzerlegungen nur die multiplikative Struktur von $\mathbb{N}$ betreffen, kann man sich fragen, ob auch ein Eindeutigkeitsbeweis möglich ist, der nur die multiplikative Struktur verwendet. Die Antwort ist nein!

Wir treffen folgende **Vereinbarungen:**

- Gleich Primfaktoren p_i in einer Primzerlegung $a = p_1 p_2 \ldots p_n$ werden zu Potenzen $p_i^{m_i}$ zusammengefasst, wobei m_i die Vielfachheit des Vorkommens von p_i als Faktor misst.
- Die Reihenfolge der Primzahlpotenzfaktoren $p_i^{m_i}$ in einer Primfaktorzerlegung von a wird gemäß der natürlichen Anordnung $2 < 3 < 5 < 7 < 11 < \ldots$ der Primzahlen normiert (also $p_1 < p_2 < \ldots$).

0.21 Folgerung: Jede natürliche Zahl $a \neq 0$ besitzt genau eine Primzerlegung

$$a = p_1^{m_1} p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}.$$

Beweis. Der Beweis ist mit der eben gemachten Vereinbarung und dem Eindeutigkeits- sowie Existenzbeweis offensichtlich. □

Mit diesen Grundlagen können wir unsere Betrachtungen, welche sich bisher auf die natürlichen Zahlen beschränkten, ohne weiteren Aufwand auf ganz $\mathbb{Z}$ ausgedehnt werden. Dazu müssen wir lediglich beachten, dass Primzahlen in $\mathbb{Z}$ gerade die Primzahlen aus $\mathbb{N}$ umfassen. Es gilt genauer $\mathbb{P}_{\mathbb{Z}} = \{\pm p | p \in \mathbb{P}\}$, dies liegt natürlich daran, dass $\{\pm 1\}$ die Einheiten des Ringes $\mathbb{Z}$ sind. D.h. auch in $\mathbb{Z}$ ist die Produktdarstellung einer beliebigen Zahl bis auf die Reihenfolge und *Assoziiertheit* eindeutig bestimmt.

0.22 Satz: (Hauptsatz der elementaren Zahlentheorie)
Jede ganze Zahl $a \neq 0$ besitzt genau eine Darstellung

$$a = \epsilon p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots p_r^{m_r} = \prod_{i=1}^{r} p_i^{m_i}.$$

mit $\epsilon = \pm 1$, Primzahlen $p_1, p_2, \ldots, p_r$ und Exponenten $m_1, m_2, \ldots, m_r$.

Beweis. Da für jede negative ganze Zahl $a \neq 0$ gilt: $a = (-1) \cdot (-a)$ mit $-a \in \mathbb{N}$. □

Es sei wiederholt, dass auch der Fall $r = 0$ des leeren Produktes 1 zugelassen ist, also $a = \pm 1$. Man nennt die durch den Hauptsatz gegebene Zerlegung von a die **kanonische Primzerlegung** von a.

Weiterhin viel Spaß mit der Mathematik!
http://www.mathematik-netz.de/ und http://www.mathering.de.

Literaturverzeichnis

[1] Algebra, Teil 1, K. Meyberg, 1980, Hanser Verlag.

[2] Algebra, Teil 2, K. Meyberg, 1980, Hanser Verlag.

[3] Elementare Zahlentheorie, R. Remmert und P. Ullrich, 1995, Birkhäuser Verlag.

[4] Deskriptive Mengenlehre, Klaus Gloede, 2006, Skriptum zur Vorlesung an der Universität Heidelberg.

[5] Kardinal- und Ordinalzahlen, Alexander Hölzle, 2008, http://www.mathematik-netz.de/pdf/KardOrd.pdf.

[6] Einführung in die Mengenlehre, Oliver Deister, 2004, Springer Verlag.