Kapitel 1

Eigenschaften der ganzen Zahlen

Aus der Veranstaltung zur Linearen Algebra ist Ihnen bekannt, dass die ganzen Zahlen $\mathbb{Z}$ mit den üblichen Verknüpfungen der Addition und Multiplikation einen nullteilerfreien, kommutativen Ring bilden, der jedoch kein Körper ist.Ein multiplikatives Inverses besitzen nur die Elemente $\{1, -1\}$. Formaler fassen wir zusammen:

- $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins.
- $(\mathbb{Z}, +, \cdot)$ besitzt keine Nullteiler.
- $\mathbb{Z}^* := \{a \in \mathbb{Z} \mid \exists b \in \mathbb{Z} : ab = ba = 1\} = \{1, -1\}$.
- $(\mathbb{Z}^*, \cdot)$ ist eine abelsche Gruppe.

Die ganzen Zahlen werden neben dem Polynomring in einer Variable über einem Körper ein grundlegendes Beispiel für viele Sachverhalte in dieser Vorlesung sein. Beim Nacharbeiten neu eingeführter Definitionen in späteren Kapiteln hilft es z.B. oft, sich zu fragen, wie das konkret für $\mathbb{Z}$ oder für $\mathbb{Q}[x]$ ausshe.

Auch die natürlichen Zahlen mit Null, $\mathbb{N}_0$ hatten wir in der Linearen Algebra kennengelernt. Hier sei insbesondere daran erinnert, dass wir das Wohlordnungsaxiom als gegeben annehmen:

Axiom 1.0.1 (Wohlordnungsaxiom) *Jede nicht-leere Teilmenge von* $\mathbb{N}_0$ *besitzt ein kleinstes Element.*

Das Wohlordnungsaxiom ist die Basis des Beweisprinzips der Vollständigen Induktion, die Sie ja bereits in der Linearen Algebra und in Mathematisches Problemlösen und Beweisen verwendet haben.

1.1 Division mit Rest

Satz 1.1.1 (Division mit Rest in $\mathbb{Z}$) *Seien $a \in \mathbb{Z}, b \in \mathbb{N}$. Dann existieren eindeutig bestimmte ganze Zahlen $q, r \in \mathbb{Z}$ mit*

$$a = q \cdot b + r \text{ und } 0 \leq r < b.$$

Die Aussage kennen sie zumindest für die natürlichen Zahlen schon aus der Grundschule. Dort wurde argumentiert, dass so lange immer b Steinchen vom Haufen mit a Steinchen weggenommen werden sollen, bis nicht mehr genug da sind. Der Grundgedanke bleibt derselbe, aber wir werden ihn im Beweis in strenger Formulierung aus dem Wohlordnungsaxiom ableiten.

Beweis:
Schritt 1: Finde einen vielversprechenden Kandidaten für r
Sei

$$M = \{a - c \cdot b \mid c \in \mathbb{Z} \text{ und } a - c \cdot b \geq 0\}.$$

M ist offensichtlich eine Teilmenge von $\mathbb{N}_0$ aufgrund der Nicht-Negativitätsbedingung. Ausserdem gilt für nicht-negative $a \in \mathbb{Z}$ einerseits

$$a = a - 0 \cdot b \in M$$

und für negative $a \in \mathbb{Z}$ andererseits

$$a - b \cdot a = \underbrace{(1-b)}_{\leq 0} \cdot \underbrace{a}_{<0} \in M,$$

weswegen M für beliebiges $a \in \mathbb{Z}$ nicht leer ist. Damit besitzt M nach dem Wohlordnungsaxiom 1.0.1 ein kleinstes Element, das wir mit r bezeichnen wollen.

Schritt 2: Zeige Eigenschaften von r und q
Für dieses r bleibt nun zu zeigen, daß $0 \leq r < b$, wobei die untere Schranke trivial erfüllt ist nach der Konstruktion von M. Würde aber $r \geq b$ gelten, so

wäre $r - b \geq 0$ und damit ein kleineres Element von M im Widerspruch zu der Wahl von r. Daher haben wir in der Tat unser gesuchtes r gefunden, das gesuchte q ist dann das c aus dem zugehörigen Ausdruck $a - c \cdot b = r$.

Schritt 3: Zeige Eindeutigkeit von (q, r)
Seien (r, q) und (r', q') nun zwei Paare, die die geforderten Eigenschaften des Satzes erfüllen und oBda $r \geq r'$. Dann gilt

$$r - r' = a - q \cdot b - (a - q' \cdot b) = (q' - q) \cdot b$$

und wegen $0 \leq r' \leq r < b$ muss damit $q' - q = 0$ gelten,was direkt $r = r'$ und $q = q'$ impliziert.

□

Korollar 1.1.2 *Seien $a, b \in \mathbb{Z}, b \neq 0$. Dann existieren eindeutig bestimmte ganze Zahlen $q, r \in \mathbb{Z}$ mit*

$$a = q \cdot b + r \text{ und } 0 \leq r < |b|.$$

Der Beweis bleibt den Studierenden als Übungsaufgabe überlassen. Ein guter Ausgangspunkt der Überlegungen ist die Division von $-a$ durch $-b$ für negatives b, aber dann muss man genau überlegen, wie man die Bedingung an r erfüllt.

Definition 1.1.3 *Das in Satz 1.1.1 eingeführte r heißt der* **Rest** *der Division von a durch b, kurz*

$$a \bmod b := r$$

das q heißt der **Quotient** *der Division von a durch b, kurz*

$$a \operatorname{div} b := q.$$

Definition 1.1.4 *Seien $a, b \in \mathbb{Z}, b \neq 0$. a heißt* **teilbar** *durch b, wenn der Rest der Division von a durch b null ist.*
Alternative Formulierungen: b **teilt** *a, b ist* **Teiler** *von a, $b \mid a$, a ist* **Vielfaches** *von b.*

Proposition 1.1.5 *Seien $a, b, c, d \in \mathbb{Z}$. Es gilt:*

a) $1 \mid a$, $a \mid a$ *und* $a \mid 0$

b) $0 \mid a \iff a = 0$

c) $a \mid b$ *und* $b \mid c \implies a \mid c$

d) $a \mid b$ *und* $c \mid d \implies ac \mid bd$

e) $\forall c \neq 0 : (a \mid b \iff ac \mid bc)$

f) $c \mid a$ *und* $c \mid b \implies c \mid (ka + mb) \forall k, m \in \mathbb{Z}$

g) $a \mid b$ *und* $b \mid a \implies a = (\pm 1)b$
(a *ist* **assoziiert** *zu* b*.)*

h) $a \mid b \implies a \mid -b$

Beweis: Alle Behauptungen sind direkte Folgerungen aus der Definition der Teilbarkeit bzw. der Division mit Rest. Daher beweisen wir hier nur den Punkt d) exemplarisch und überlassen die anderen den Studierenden zur Übung:

$$\begin{aligned}(a \mid b \text{ und } c \mid d) &\implies \exists k, m \in \mathbb{Z} : b = ka \text{ und } d = mc \\ &\implies bd = (ka)(mc) \overset{(AG)}{=} kamc \overset{(KG)}{=} kmac \overset{(AG)}{=} (km)(ac) \\ &\implies ac \mid bd\end{aligned}$$

□

Sollten Sie noch Kontakt zu Ihrem Abgabepartner aus der Linearen Algebra haben und mit diesem/dieser gut zusammengearbeitet haben, so empfiehlt es sich in der gegenwärtigen Situation, sich gegenseitig per Mail / StudIP / WhatsApp / Skype / o.ä. abwechselnd die Argumente der einzelnen Punkte zu erklären, damit Sie sich in das derzeit erzwungene mathematische Zusammenarbeiten auf elektronischem Weg einfinden.

Definition 1.1.6 *Seien* $a, b \in \mathbb{Z}$*.*

a) Gilt $c \mid a$ *und* $c \mid b$ *für ein* $c \in \mathbb{Z}$*, so heißt* c *ein* **gemeinsamer Teiler** *von* a *und* b*.*

b) $c \in \mathbb{Z}$ *heißt ein* **größter gemeinsamer Teiler** *von* a *und* b*, falls gilt:*

(i) $c \mid a$ *und* $c \mid b$

(ii) Für $d \in \mathbb{Z}$ *gilt:* $((d \mid a \text{ und } d \mid b) \Longrightarrow d \mid c)$

c) a *und* b *heißen* **teilerfremd**, *falls* ± 1 *die einzigen gemeinsamen Teiler von* a *und* b *sind.*

Notation 1.1.7 *Gerne spricht man auch von* **dem** *größten gemeinsamen Teiler von* a *und* b *statt von* **einem** *größten gemeinsamen Teiler von* a *und* b. *In diesem Fall wählt man aus der Menge der beiden größten gemeinsamen Teiler den positiven aus, was wir im Folgenden auch tun werden. Diesen bezeichnen wir mit* $\mathrm{ggT}(a, b)$.

Bisher haben wir den größten gemeinsamen Teiler definiert, aber noch nicht bewiesen, dass er auch existiert. Dies werden wir erst nach der Betrachtung erster Eigenschaften des ggT nachholen, da wir einige davon benötigen. Insbesondere sind zum jetzigen Zeitpunkt alle Aussagen der folgende Proposition zu lesen mit dem Zusatz 'unter der Voraussetzung, dass $\mathrm{ggT}(a, b)$ existiert, existieren auch die anderen angegebenen ggT'.

Proposition 1.1.8 (Eigenschaften des ggT**)** *Seien* $a, b \in \mathbb{Z}$. *Es gilt:*

a) $\mathrm{ggT}(b, a) = \mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$

b) $b \mid a \Longrightarrow \mathrm{ggT}(a, b) = |b|$

c) $\mathrm{ggT}(a, 0) = |a|$

d) $\mathrm{ggT}(a, b) = \mathrm{ggT}(a \bmod b, b)$

e) $\mathrm{ggT}\left(\frac{a}{\mathrm{ggT}(a,b)}, \frac{b}{\mathrm{ggT}(a,b)}\right) = 1$

Beweis: Hier nur ein Hinweis zum Beweis, jedoch keine Ausführung bis ins Detail: Alle Aussagen folgen direkt aus der Definition des ggT. Dabei nutzt man aus, dass bei Gleichheit der Mengen aller gemeinsamen Teiler zweier Zahlen auch der ggT übereinstimmt. In d) verwendet man zusätzlich die Definition der Division mit Rest, in e) die Tatsache, dass für jeden gemeinsamen Teiler d von $\frac{a}{\mathrm{ggT}(a,b)}$ und $\frac{b}{\mathrm{ggT}(a,b)}$ auch $d \cdot \mathrm{ggT}(a, b)$ gemeinsamer Teiler von a und b ist.

□

Satz 1.1.9 (Existenz des $\mathrm{ggT}(a,b)$**)** *Seien* $a, b \in \mathbb{Z}, b \neq 0$. *Dann existiert* $\mathrm{ggT}(a,b)$.

Diese Aussage kann man auf verschiedene Weise beweisen. Man kann über den Durchschnitt der Mengen der Teiler von a und b argumentieren oder einen algorithmischen Beweis führen, den wir später in allgemeinerem Kontext kennenlernen werden. Hier verwenden wir aus didaktischen Gründen einen Beweis, der nochmals das Wohlordnungsaxiom verwendet.

Beweis: Da Teiler einer ganzen Zahl nach 1.1.5 auch stets Teiler von deren additivem Inversen sind, reicht es im Beweis aus, sich auf nicht-negative a und b zu beschränken. Wir werden durch Widerspruchsbeweis zu unserem Ziel gelangen.
Nehmen wir also an, dass es Zahlenpaare $(a,b) \in \mathbb{N}_0 \times \mathbb{N}$ gibt mit $a < b$, für die es keinen ggT gibt. Nach Axiom 1.0.1 hat die nach Annahme nicht-leere Menge in solchen Paaren auftretender erster Einträge ein kleinstes Element a_0 und nochmals nach Axiom 1.0.1 die Menge aller in solchen Paaren mit erstem Eintrag a_0 auftretenden zweiten Einträge ein kleinstes Element b_0.
Da $\mathrm{ggT}(0, b_0) = |b_0|$ nach 1.1.8,c) und damit existent, ist $a_0 > 0$. Betrachten wir nun $\mathrm{ggT}(b_0 \bmod a_0, a_0)$. Wir wissen, dass nach 1.1.1 $(b_0 \bmod a_0) < a_0$. Damit kann $b_0 \bmod a_0$ nach der Minimalität von a_0 nicht in einem Paar auftreten, für das kein größter gemeinsamer Teiler existiert. Also existiert $\mathrm{ggT}(b_0 \bmod a_0, a_0)$. Jeder gemeinsame Teiler von $b_0 \bmod a_0$ und a_0 ist aber auch gemeinsamer Teiler von a_0 und b_0 und umgekehrt, aufgrund von

$$b_0 = (b_0 \operatorname{div} a_0) \cdot a_0 + (b_0 \bmod a_0).$$

Natürlich bleiben auch die Teilbarkeiten zwischen den gemeinsamen Teilern dabei unberührt, weswegen $\mathrm{ggT}(a_0, b_0)$ mit $\mathrm{ggT}(b_0 \bmod a_0, a_0)$ übereinstimmt und insbesondere existiert im Widerspruch zur Wahl von a_0 und b_0.

□

Bemerkung 1.1.10 *Betrachtet man mehr als* 2 *Zahlen, sagen wir* $a_1, \ldots, a_k \in \mathbb{Z}$ *so kann man sich auch die Fragen nach dem grössten gemeinsamen Teiler alle Zahlen stellen. Diesen kann man induktiv definieren als*

$$\mathrm{ggT}(a_1, \ldots, a_k) := \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{k-1}), a_k).$$

Mit dieser Verallgemeinerung und ihren Eigenschaften werden Sie sich auf Übungsblatt 01 noch näher beschäftigen.

Satz 1.1.11 (Bézout-Identität, elementare Version) *Seien $a, b \in \mathbb{Z}, b \neq 0$. Dann existieren $x, y \in \mathbb{Z}$, so dass*

$$\mathrm{ggT}(a, b) = xa + yb.$$

Insbesondere ist $\mathrm{ggT}(a, b)$ die kleinste natürliche Zahl, die als $\mathbb{Z}$-Linearkombination von a und b dargestellt werden kann.

Beweis: Sei $M = \{c \in \mathbb{N} \mid \exists k, m \in \mathbb{Z} : c = ka + mb\}$. Die Menge ist nicht leer, da $|b| \in M$, so dass sie nach 1.0.1 ein minimales Element $d = xa + yb$ hat.
Schritt 1: d teilt a und b
Betrachte die Division a durch d:

$$a = q \cdot d + r \text{ für ein } q \in \mathbb{Z} \text{ und ein } 0 \leq r < d.$$

Dann ist

$$r = a - q \cdot (xa + yb) = (1 - qx)a + qyb \in M \cup \{0\}$$

und wegen der Minimalität von d in M gilt damit $r = 0$. Also gilt $d \mid a$ und wegen der Symmetrie der Situation auch $d \mid b$.
Schritt 2: $d = \mathrm{ggT}(a, b)$ Sei $c \in \mathbb{N}$ ein weiterer gemeinsamer Teiler von a und b, so gilt $c \mid xa + yb$, d.h. $c \mid d$, weswegen d größter gemeinsamer Teiler von a und b ist.

□

Bemerkung 1.1.12 *Der Satz 1.1.11 impliziert auch, dass alle $\mathbb{Z}$-Linearkombinationen von a und b selbst wieder Vielfache von $d = \mathrm{ggT}(a, b)$ sind. Denn gäbe es eine Linearkombination, die kein Vielfaches von d wäre, so ließe sich auch deren größter gemeinsamer Teiler mit d, der echt kleiner als d wäre, als Linearkombination aus a und b darstellen im Widerspruch zur Minimalität von d in M. Es gilt also:*

$$\{xa + yb \mid x, y \in \mathbb{Z}\} = \{zd \mid z \in \mathbb{Z}\}$$

Die bisher betrachteten Eigenschaften werden wir später in allgemeinerem Kontext wiedersehen und dort auch nochmals und dann mit konstruktiver Herangehensweise beweisen. Trotzdem ist es gut, die Überlegungen hier sorgfältig durchzudenken und die hier behandelten Tatsachen als Beispielvorrat für spätere Aussagen im Kopf zu behalten.

1.2 Ideale in $\mathbb{Z}$

Die in Bemerkung 1.1.12 aufgetauchte Menge ist ein erstes Beispiel einer neuer mathematischen Struktur, nämlich eines Ideals. Ideale können in beliebigen Ringen betrachtet werden. Allerdings haben Ideale in $\mathbb{Z}$ besonders schöne Eigenschaften, wie wir gleich sehen werden, so dass sie gut für den ersten Einstieg geeignet sind.

Definition 1.2.1 *Eine nicht-leere Teilmenge $I \subseteq \mathbb{Z}$ heißt* **Ideal** *in $\mathbb{Z}$, kurz $I \trianglelefteq \mathbb{Z}$, falls gilt:*

a) $\forall a, b \in I : a + b \in I$

b) $\forall a \in I, \forall r \in \mathbb{Z} : ar \in I$

Bemerkung 1.2.2 *Die Menge*

$$M = \{xa + yb \mid x, y \in \mathbb{Z}\} = \{zd \mid z \in \mathbb{Z}\}$$

ist ein Ideal, denn schon aus der jeder der beiden Beschreibungen der Menge wird klar, dass Summen und ganzzahlige Vielfache von Elementen von M wieder Elemente von M sind. Es handelt sich hierbei augenscheinlich um das kleinste Ideal, das a und b enthält, aber auch um das kleinste Ideal, das d enthält.

Definition 1.2.3 *Für $a_1, \ldots, a_n \in \mathbb{Z}$ heisst*

$$I := \langle a_1, \ldots, a_n \rangle := \{\sum_{i=1}^{n} k_i a_i \mid k_1, \ldots, k_n \in \mathbb{Z}\} \trianglelefteq \mathbb{Z}$$

das von $a_1, \ldots, a_n$ **erzeugte Ideal**, *$a_1, \ldots, a_n$ werden als* **Erzeuger** *von I bezeichnet.*

Definition 1.2.4 *Ein Ideal, das sich in der Form $I = \langle a_1 \rangle \trianglelefteq \mathbb{Z}$ schreiben läßt, wird als* **Hauptideal** *in $\mathbb{Z}$ bezeichnet.*

Bemerkung 1.2.5 *Wir werden später sehen, dass sich die Definition eines Ideals und auch die eines Hauptideals nahezu wörtlich auf beliebige kommutative Ringe mit 1 übertragen lassen. Ein kommutativer, nullteilerfreier Ring mit Eins, in dem jedes Ideal ein Hauptideal ist, wird als* **Hauptidealring** *bezeichnet werden. Mit diesem Ausblick sagt der folgende Satz aus, dass $\mathbb{Z}$ ein Hauptidealring ist.*

Satz 1.2.6 *Jedes Ideal $I \trianglelefteq \mathbb{Z}$ ist ein Hauptideal.*

Ehe wir diesen Satz beweisen, formulieren wir 1.1.11 neu in der Sprache der Ideale in $\mathbb{Z}$. Hierzu ist kein Beweis notwendig, da es sich lediglich um die Verwendung einer neuen Schreibweise für eine bereits bewiesene Tatsache handelt. Diese neue Schreibweise andererseits hilft uns, den obigen Satz in kompakter Form zu beweisen.

Satz 1.2.7 *Seien $a, b \in \mathbb{Z}, b \neq 0$. Dann gilt:*

$$\langle a, b\rangle = \langle \mathrm{ggT}(a, b)\rangle.$$

Beweis:(von Satz 1.2.6) Sei $I \trianglelefteq \mathbb{Z}$ ein beliebiges Ideal. Da I nicht leer ist, existiert mindestens ein $d_0 \in I$ und oBdA ist $d_0 \geq 0$. Ist $I = \langle d_0\rangle$, so ist I Hauptideal. Ansonsten ist $\langle d_0\rangle \subsetneq I$ und es existiert ein $a_0 \in I \setminus \langle d_0\rangle$. Damit ist $\langle d_0, a_0\rangle \subseteq I$, was nach 1.2.7 bedeutet, dass $\langle d_1\rangle \subseteq I$, wobei $d_1 = \mathrm{ggT}(d_0, a_0)$. Insbesondere ist aber wegen $d_1 \in I \setminus \langle d_0\rangle$ die positive ganze Zahl d_1 echt kleiner als d_0. Diese Konstruktion können wir nun iterieren: Ist im i-ten Durchlauf der Konstruktion $\langle d_i\rangle \subsetneq I$, so wird ein Element $a_i \in I \setminus \langle d_i\rangle$ sowie $d_{i+1} = \mathrm{ggT}(d_i, a_i)$ bestimmt, was eine Kette positiver ganzer Zahlen

$$d_0 > d_1 > \ldots > d_{i+1} > \ldots$$

erzeugt. Da aber nur endlich viele positive ganze Zahlen kleiner als d_0 sind, kann diese Kette irgendwann nicht mehr fortgesetzt werden, sagen wir bei einem d_n. Das bedeutet insbesondere, dass $I = \langle d_n\rangle$ erfüllt ist. I ist somit Hauptideal mit Erzeuger d_n.

□

Hier noch eine andere naheliegend erscheinende Aussage, die wir explizit beweisen werden. Sie stammt schon aus der griechischen Antike und dient uns hier als Übergang zu einer anderen zentralen Tatsache über die ganzen Zahlen, dem Fundamentalsatz der Arithemtik.

Lemma 1.2.8 (Euklid) *Seien $a, b, c \in \mathbb{Z}$ mit $a \neq 0$, $a \mid bc$ und $\mathrm{ggT}(a, b) = 1$. Dann gilt*

$$a \mid c.$$

Beweis: Ist $c = 0$, so ist die Aussage trivial, da jede ganze Zahl Null teilt. Wir beschränken uns ab jetzt also auf den Fall $c \neq 0$.
Nach Satz 1.1.11 impliziert $\mathrm{ggT}(a, b) = 1$ die Exisitenz von $x, y \in \mathbb{Z}$ mit

$$xa + yb = 1.$$

Multipliziert mit c liefert diese Gleichung:

$$xac + ybc = c.$$

Da a nun offensichtlich Teiler von xac ist und nach Voraussetzung Teiler von ybc, ist a auch Teiler von c.

□

Definition 1.2.9 *Eine Zahl $p \in \mathbb{N}$ heißt* **Primzahl**, *wenn sie genau zwei positive Teiler besitzt, nämlich 1 und p. Eine Zahl $n \in \mathbb{N}$ mit $n \geq 2$, die keine Primzahl ist, heißt* **zusammengesetzte Zahl**.

Bemerkung 1.2.10 *Ist n eine zusammengesetzte Zahl, so besitzt n noch mindestens einen Teiler $1 < n_1 < n$ und läßt sich daher als Produkt $n = n_1 \cdot \frac{n}{n_1}$ schreiben, wobei $\frac{n}{n_1}$ eine ganze Zahl ist.*

Korollar 1.2.11 *Sei p eine Primzahl und seien $a, b \in \mathbb{Z}$. Dann gilt:*

$$p \mid ab \Longrightarrow p \mid a \text{ oder } p \mid b.$$

Dies ist eine direkte Folgerung aus dem Lemma von Euklid und wird oft auch selbst als Lemma von Euklid bezeichnet.

Satz 1.2.12 (Fundamentalsatz der Arithmetik) *Jede natürliche Zahl $n \geq 2$ kann als Produkt von Primzahlen dargestellt werden, d.h. zu jedem $n \geq 2$ existieren $k \in \mathbb{N}$ sowie $p_1, \ldots, p_k$ (nicht notwendigerweise verschiedene) Primzahlen mit*

$$n = \prod_{i=1}^{k} p_i.$$

Die Faktorisierung ist bis auf Reihenfolge eindeutig.

Beweis: Wir führen den Beweis der Existenz der Zerlegung durch Induktion nach n:

Induktionsanfang: $n = 2$
$n = 2$ ist selbst Primzahl, so dass $n = p_1$ mit $p_1 = 2$ die gesuchte Zerlegung ist.

Induktionsvoraussetzung: n
Jede natürliche Zahl $2 \leq m \leq n$ besitzt eine Zerlegung in Primfaktoren.

Induktionsschritt: $n \mapsto n + 1$
Ist $n + 1$ Primzahl, so ist die Zerlegung in Primfaktoren bereits gefunden. Wir betrachten daher ab jetzt den Fall, dass $n + 1$ zusammengesetzt ist. Als zusammengesetzte Zahl hat $n + 1$ mindestens einen echten Teiler $1 < m_1 < n + 1$ und läßt sich daher schreiben als

$$n + 1 = m_1 \cdot m_2 \text{ mit } m_2 := \frac{n+1}{m_1} \in \mathbb{N}.$$

Für die natürlichen Zahlen $m_1, m_2 < n + 1$ existiert nach Induktionsvoraussetzung eine Zerlegung in Primfaktoren

$$m_1 = \prod_{i=1}^{k_1} p_{1,i} \text{ und } m_2 = \prod_{i=1}^{k_2} p_{2,i}$$

weswegen auch gilt

$$n + 1 = \prod_{j=1}^{2} \left(\prod_{i=1}^{k_j} p_{j,i} \right),$$

was die gesuchte Zerlegung von $n + 1$ in Primfaktoren liefert.

Es bleibt nun noch die Eindeutigkeit der Zerlegung bis auf Reihenfolge zu zeigen. Auch hier gehen wir wieder per Induktion nach n vor.

Induktionsanfang: $n = 2$
$n = 2$ ist als Primzahl ihre eigene Zerlegung, die offensichtlich eindeutig ist.

Induktionsvoraussetzung: n
Die Zerlegung jeder natürlichen Zahl $2 \leq m \leq n$ in Primfaktoren ist bis auf

Reihenfolge eindeutig.

Induktionsschritt: $n \mapsto n+1$
Seien nun

$$n+1 = \prod_{i=1}^{k} p_i \text{ und } n+1 = \prod_{j=1}^{r} q_j$$

zwei Zerlegungen von $n+1$ in Primfaktoren. Dann ist die Primzahl p_k nach dem Korollar zum Lemma von Euklid 1.2.11 ein Teiler eines der Primfaktoren q_j und damit $p_k = q_j$. Ohne Beschränkung der Allgemeinheit ist dieses $j = r$. Damit haben wir einen Primfaktor in der Zerlegung identifiziert und können ihn in beiden Produkten herausteilen;

$$\prod_{i=1}^{k-1} p_i = \frac{n+1}{p_k} = \prod_{j=1}^{r-1} q_j.$$

Ist $\frac{n+1}{p_k} = 1$, so war $n+1$ bereits eine Primzahl und es ist nichts mehr zu zeigen. Andernfalls die Zerlegung natürlichen Zahl $1 < \frac{n+1}{p_k} < n+1$ nach Induktionsvoraussetzung bis auf Reihenfolge eindeutig, so dass damit auch die Eindeutigkeit der Zerlegung von $n+1$ bis auf Reihenfolge bewiesen ist.

□