§1 Teiler, Primzahlen und Hauptsatz der Arithmetik

1. Erinnerung: Wir betrachten die Menge der natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ und die Menge der ganzen Zahlen $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ mit den üblichen Operationen $+, \cdot$, der Anordnung $\leq$ sowie der Absolutbetrag $|z| = \max\{z, -z\}$.

In $\mathbb{N}$ ist die Subtraktion nur eingeschränkt möglich, $3 + x = 2$ hat keine Lösung x in $\mathbb{N}$.
In $\mathbb{Z}$ ist die Subtraktion uneingeschränkt möglich, aber nicht die Division, $3y = 2$ hat keine Lösung y in $\mathbb{Z}$.

Es gelten aber die Kürzungsregeln:

- $a + x = a + y \Rightarrow x = y$
- $b \neq 0,\ bx = by \Rightarrow x = y$

2. Wiederholung: Induktion und Wohlordnung

Ein wichtiges Beweishilfsmittel ist das Induktionsprinzip.

1. Induktionsprinzip Ist $S \subseteq \mathbb{N}$ Teilmenge mit

(i) $0 \in S$

(ii) $s \in S \Rightarrow s+1 \in S$

so gilt $S = \mathbb{N}$. "Alle natürlichen Zahlen erhält man, wenn man bei Null anfängt zu zählen".

Das 1. Induktionsprinzip folgt aus der Konstruktion der Menge $\mathbb{N}$ in der Mengenlehre (→ Peano-Axiome). Aus ihm folgt zum weiteren Beweishilfsmittel.

Das Wohlordnungsprinzip Ist $S \subseteq \mathbb{N}$ Teilmenge mit $S \neq \emptyset$, so hat S ein einziges kleinstes Element $s_0 = \min(S)$

Beweis (IP1 ⇒ WP) Sei $\emptyset \neq S \subseteq \mathbb{N}$ Teilmenge.
Sei $T = \{t \in \mathbb{N} \mid \text{für jedes } s \in S \text{ gilt } t \leq s\}$.
Es folgt $0 \in T$ (für alle $s \in S$ gilt $0 \leq s$).
Für $s \in S$ gilt $s+1 \notin T$ (denn $s+1 \not\leq s$),
also gilt $T \neq \mathbb{N}$

Nach IP1 gibt es also $s_0 \in T$ mit $s_0+1 \notin T$.

Beh: $s_0 \in S$.

Denn sonst wäre $s_0 < s$ für alle $s \in S$, damit $s_0+1 \leq s$ für alle $s \in S \Rightarrow s_0+1 \in T$ ↯ □

Da $s_0 \in T$ gilt $s_0 \leq s$ für alle $s \in S$, d.h. s_0 ist ein kleinstes Elem in S. Wäre $s_1 \in S$ ein weiteres kleinstes Elem in S, so wäre $s_0 \leq s_1 \leq s_0$ $\Rightarrow s_1 = s_0$, also ist s_0 eindeutig bestimmt. □

2. Induktives Prinzip Ist $S \subseteq \mathbb{N}$ eine Teilmenge mit

(i) $0 \in S$

(ii) für alle $t < s$ gilt $t \in S \Rightarrow s \in S$

so gilt $S = \mathbb{N}$

Beweis (WP $\Rightarrow$ IP2)

Angenommen, $S \subseteq \mathbb{N}$ hat Eigenschaften (i) und (ii), aber $S \neq \mathbb{N}$. Setze $R = \mathbb{N} - S$. Dann ist $R \neq \emptyset$, also existiert nach WP $r = \min(R)$. Wegen $0 \in S$ ist $r > 0$. Für alle $t \in \mathbb{N}$ mit $t < r$ gilt $t \in S$ (weil $r = \min(\mathbb{N}-S)$) $\overset{(ii)}{\Rightarrow} r \in S$. Aber $r \in R = \mathbb{N}-S$ ↯

□

Vorsicht: (IP1), (WP) und (IP2) gelten für Teilmengen von $\mathbb{N}$, aber nicht unbedingt für Teilmengen von $\mathbb{Z}$. So hat zum Beispiel die Menge $S = \mathbb{Z}$ kein kleinstes Element.

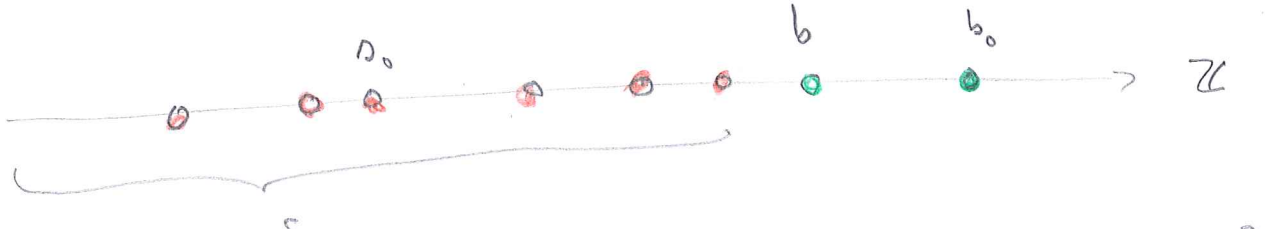
Es gibt aber folgendes hilfreiches Ergebnis. #

3. Lemma Sei $S \subseteq \mathbb{Z}$ eine Teilmenge, $S \neq \emptyset$.

Falls S eine obere (bzw. untere) Schranke hat, so hat S ein größtes Element $\max(S)$ (bzw. ein kleinstes Element $\min(S)$).

Beis: Sei $s_0 \in S$, sei $b_0 \in \mathbb{Z}$ eine obere Schranke für S (d.h. $b_0 \geq s$ für alle $s \in S$).

Dann ist jede obere Schranke b von S von der Form $b = s_0 + t$, für ein $t \in \mathbb{N}$, dem $b \geq s_0$.



Setze $r = \min \{ t \in \mathbb{N} \mid s_0 + t \text{ ist obere Schranke für } S \}$

$\neq \emptyset$

Set $m = s_0 + r$. Beh: $m = \max(S)$.

Nach Konstruktion gilt $s \leq m$ für alle $s \in S$.

Wäre $m \notin S$, so hätten wir $s < m$ für alle $s \in S$

$\Rightarrow$ $s \leq m-1$ für alle $s \in S$ $\Rightarrow$ $m-1$ obere Schranke,

$m - 1 = s_0 + (r-1)$ ↯ zur Wahl von r.

Also gilt $m \in S \Rightarrow m = \max(S)$.

Für das Minimum und untere Schranke $a_0 \in \mathbb{Z}$ betrachte

$$R = \{ t \in \mathbb{N} \mid s_0 - t \text{ ist untere Schranke von } S \}$$

$\neq \emptyset$

$r = \min(R)$ und zeige, dass $\min(S) = s_0 - r$ gilt

(ähnlich wie oben). □

4. Beispiel eines Beweis mit (WP): "Prinzip des kleinsten Verbrechers"

Jedes Briefporto von mindestens 8 Cent läßt sich mit 3- und 5-Cent Marken genau erzielen.

Beweis: Sei $P = \{ a \cdot 3 + b \cdot 5 \mid a, b \in \mathbb{N} \text{ und } a \cdot 3 + b \cdot 5 \geq 8 \}$

Zu zeigen: $P = \{ t \in \mathbb{N} \mid t \geq 8 \}$

Wäre das falsch, so gäbe es ein kleinstes

Element $t \in \mathbb{N}$ mit $t \geq 8$ und $t \notin P$.

Es gilt $8 = 5+3$, $9 = 3 \cdot 3$, $10 = 2 \cdot 5 \Rightarrow t \geq 11$.

Folglich ist $t - 3 \in P$ (weil t minimal)

$t-3 = 3\cdot a + 5\cdot b$. Aber dann $t = (3+1)a + 5\cdot b \in P$ ↯

□

Noch eine allgemeine Überlegung betrachten wir Teilbarkeit.

5. Def Seien $a, b \in \mathbb{Z}$ beliebig. Falls es $m \in \mathbb{Z}$ gibt mit $a \cdot m = b$, so heißt a Teiler von b und man schreibt

$a \mid b$ "a teilt b".

Wenn es kein solches m gibt, schreibt man

$a \nmid b$ "a teilt b nicht".

Bsp $3 \mid 21$ und $3 \nmid 22$.

Es gelten folgende Rechenregeln für Teilbarkeit.

Sei $a, b, c \in \mathbb{Z}$

(i) $\pm 1 \mid a$, $a \mid \pm a$, $-a \mid b$

(ii) $a \mid b$ und $b \mid c \Rightarrow a \mid c$

(iii) $a \mid b$ und $b \mid a \Rightarrow a = \pm b$

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

(v) $a\neq 0$ und $ab|ac \Rightarrow b|c$

Beis: (i) ist klar nach Definition

(ii) $a\cdot m=b \quad b\cdot n=c \Rightarrow a\cdot m\cdot n=c$

(iv) $a\cdot m=b \quad a\cdot n=c \Rightarrow a(m\pm n)=b\pm c$

(iii) $a\cdot m=b \quad b\cdot n=a \Rightarrow a=m\cdot n\cdot a$ $\quad b=0$ fertig.

$\Rightarrow a=0$ oder $m\cdot n=1$

Wenn $a=0$, dann $b=0$ $\rightsquigarrow$ fertig.

Wenn $m\cdot n=1$, dann $m,n\neq 0 \rightsquigarrow |m|,|n|\geq 1$

$1=|m|\cdot|n| \Rightarrow |m|=1=|n| \rightsquigarrow m=\pm 1, n=\pm 1$ fertig.

(v) $abm=ac$ und $a\neq 0 \overset{\text{Kürzen}}{\rightsquigarrow} bm=c$

$\Rightarrow b|c$ □

6. Satz (vom Teilen mit Rest)

Sind $a,b\in\mathbb{Z}$ mit $b\neq 0$. Dann gibt es eindutig Zahlen $r,s\in\mathbb{Z}$ mit

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

↑ Rest

Beis Eindeutigkeit

Angenn, $a = b \cdot s + r = b \cdot s' + r'$, $0 \le r, r' < |b|$.

Es folgt $b(s-s') = r'-r$ und $|r'-r| < |b|$

Folglich $|s-s'| < 1$, also $s = s'$

$\Rightarrow r = r'$

Existenz Sei $T = \{ u \cdot b \mid u \in \mathbb{Z} \text{ und } ub \le a \}$

Für $b > 0$ wähle $u \in \mathbb{Z}$ mit $u \le \frac{a}{b}$ so $ub \le a$

Für $b < 0$ wähle $u \in \mathbb{Z}$ mit $u \ge \frac{a}{b}$ so $ub \le a$

$\Rightarrow T \neq \emptyset$. Sei $t = \max(T)$, $t = s \cdot b \le a$

für ein $s \in \mathbb{Z}$. Also $a = s \cdot b + r$ für ein $r \in \mathbb{N}_0$.

Wäre $r \ge |b|$, so $a = \underbrace{s \cdot b + |b| b}_{(s+\varepsilon)b > s \cdot b} + r'$ $0 \le r' < r$

$\varepsilon = \begin{cases} 1 & b > 0 \\ -1 & b < 0 \end{cases}$

also $(s+\varepsilon)b \in T$ ↯, da $(s+\varepsilon)b > s \cdot b$.

Damit $0 \le r < |b|$ □

7. Satz Sei $H \le \mathbb{Z}$ eine Teilmge mit

(i) $H \neq \emptyset$

(ii) für alle $a, b \in H$ gilt $a - b \in H$.

Dann gibt es genau ein $d \in \mathbb{N}$ mit

$H = d \cdot \mathbb{Z} = \{ d \cdot z \mid z \in \mathbb{Z} \}$.

Beweis Sei $h \in H$ beliebig. Es folgt $0 = h - h \in H$, damit $-h = 0 - h \in H$ sowie $h + h = h - (-h) \in H$.
Folglich $h \cdot \mathbb{Z} \subseteq H$.
Falls $H = \{0\}$, so $H = 0 \cdot \mathbb{Z}$ fertig.
Falls $H \neq \{0\}$, so gibt es nach der vor. Überlegung $h \in H$ mit $h > 0$. Setze $d = \min\{h \in H \mid h > 0\} > 0$ es folgt $d \cdot \mathbb{Z} \subseteq H$.
Für $h \in H$ beliebig gibt es nach §1.6 Zahl $r, s \in \mathbb{Z}$ mit $h = s \cdot d + r$, $0 \leq r < d$.
Es folgt $r = h - s \cdot d \in H$, also $r = 0$ $\rightsquigarrow$ $h = s \cdot d$ $h \in d\mathbb{Z}$. Damit $H \subseteq d \cdot \mathbb{Z}$, insgesamt $H = d \cdot \mathbb{Z}$.

Zur Eindeutigkeit: angenom. $d, \tilde{d} \in \mathbb{N}$ mit $H = d \cdot \mathbb{Z} = \tilde{d} \cdot \mathbb{Z}$. Es folgt $d \mid \tilde{d}$ und $\tilde{d} \mid d$ $\rightsquigarrow$ $d = \pm \tilde{d}$ nach §1.5 $\rightsquigarrow$ $d = \tilde{d}$ mit $d, \tilde{d} \geq 0$ □

8. Korollar Sei $n \geq 1$, seien $a_1, \ldots, a_n \in \mathbb{Z}$. Setze

$$(a_1, \ldots, a_n)_{\mathbb{Z}} = \left\{ a_1 z_1 + \ldots + a_n z_n \;\middle|\; z_1, \ldots, z_n \in \mathbb{Z} \right\}$$

die Menge der ganzzahligen Linearkombinationen der $a_1, \ldots, a_n$. Dann gibt es genau ein

$d \in \mathbb{N}$ mit

$(a_1, \dots, a_n)_{\mathbb{Z}} = d \cdot \mathbb{Z} = (d)_{\mathbb{Z}}$ und wir definieren

den <u>größten gemeinsamen Teiler</u>

$$d = ggT(a_1, \dots, a_n).$$

<u>Beweis</u> Die Menge $H = (a_1, \dots, a_n)_{\mathbb{Z}}$ erfüllt die Bedingungen (i) und (ii) aus §1.7. □

In der Schule wird der ggT anders definiert, aber unsere Definition ist vorteilhafter und liefert das gleiche Ergebnis:

9. <u>Lemma</u> Sei $a_1, \dots, a_n \in \mathbb{Z}$, $n \geq 1$, und sei $d = ggT(a_1, \dots, a_n)$. Dann gilt:

(i) $d \mid a_k$ für alle $k = 1, \dots, n$

(ii) Ist $b \in \mathbb{Z}$ und gilt $b \mid a_k$ für alle $k = 1, \dots, n$, so folgt $b \mid d$.

<u>Beweis</u> (i) Für jedes k gilt $a_k = 1 \cdot a_k \in (a_1, \dots, a_n)_{\mathbb{Z}}$

$\Rightarrow a_k = d \cdot z$ für ein $z \in \mathbb{Z} \Rightarrow d \mid a_k$.

(ii) Angenommen, $b \mid a_1, \dots, b \mid a_n$. Es folgt $b \mid h$ für jedes $h \in (a_1, \dots, a_n)_{\mathbb{Z}} \Rightarrow b \mid d$ □

Bem (i) Wenn $0 = ggT(a_1, \dots, a_n)$, so folgt $a_1 = \dots = a_n = 0$.

(ii) Wenn $d = ggT(a_1, \dots, a_n)$, so gibt es also $z_1, \dots, z_n \in \mathbb{Z}$ mit $d = a_1 z_1 + \dots + a_n z_n$, d.h. d ist ganzzahlige Linearkombination der $a_1, \dots, a_n$. Das folgt aus unserer Def. des ggT direkt (aber nicht aus der Definition in der Schule).

(iii) Ist $n \geq 3$ und $1 < k < n$, so gilt

$$ggT(a_1, \dots, a_n) = ggT(ggT(a_1, \dots, a_k), ggT(a_{k+1}, \dots, a_n))$$

denn: $d = ggT(a_1, \dots, a_n)$

$d_1 = ggT(a_1, \dots, a_k)$

$d_2 = ggT(a_{k+1}, \dots, a_n)$

$$\Rightarrow d\cdot\mathbb{Z} = (a_1, \dots, a_n)_{\mathbb{Z}}$$
$$= (a_1, \dots, a_k)_{\mathbb{Z}} + (a_{k+1}, \dots, a_n)_{\mathbb{Z}}$$
$$= d_1\cdot\mathbb{Z} + d_2\mathbb{Z} = (d_1, d_2)_{\mathbb{Z}}$$

□

10. **Def** Die Zahlen $a_1, \dots, a_n \in \mathbb{Z}$ heißen **teilerfremd** oder **coprim**, wenn gilt

$$ggT(a_1, \dots, a_n) = 1.$$

In dem Fall sind (nach §1.9) ± 1 die einzigen Zahlen, die **alle** $a_1, \dots, a_n$ teilen.

Satz Sei $a_1, \dots, a_n \in \mathbb{Z}$. Dann sind äquivalent:

(i) $ggT(a_1, \dots, a_n) = 1$

(ii) es gibt $z_1, \dots, z_n$ mit

$$1 = a_1 z_1 + \dots + a_n z_n$$

Beweis (i) $\Rightarrow$ (ii) nach §1.9.

(ii) $\Rightarrow$ (i) $1 = a_1 z_1 + \dots + a_n z_n \Rightarrow 1 \in d \cdot \mathbb{Z}$

für $d = ggT(a_1, \dots, a_n) \Rightarrow d \mid 1$ und $1 \mid d$

$\Rightarrow d = 1$ □

Korollar A Ist $a_1, \dots, a_n \in \mathbb{Z}$ und ist

$d = ggT(a_1, \dots, a_n) \neq 0$, so setze $a_k = d \cdot \tilde{a}_k$.

Dann ist $ggT(\tilde{a}_1, \dots, \tilde{a}_n) = 1$.

Beis $d = a_1 z_1 + \dots + a_n z_n$ für geeignete $z_1, \dots, z_n \in \mathbb{Z} \rightsquigarrow d = d \cdot (\tilde{a}_1 z_1 + \dots + \tilde{a}_n z_n)$

$d \neq 0$
$\rightsquigarrow 1 = \tilde{a}_1 z_1 + \dots + \tilde{a}_n z_n$ □

Korollar B Angenommen, $a, b, c \in \mathbb{Z}$ mit $ggT(a,b) = 1$ und $a \mid bc$. Dann folgt $a \mid c$.

Beis Es gibt $x, y \in \mathbb{Z}$ mit $ax + by = 1$, also

$c = cax + cby = a(cx) + (bc) \cdot y$

$\Rightarrow a \mid c$ □

Korollar C Angenommen, $a, b, c \in \mathbb{Z}$ mit

$1 = ggT(a,b) = ggT(a,c)$, so folgt $ggT(a, bc) = 1$

Beis Es gibt $x, y, u, v \in \mathbb{Z}$ mit

$1 = ax + by = au + cv \rightsquigarrow$

$1 = (ax + by)(au + cv) = a(uxa + cvx + byu) + bc(vy)$

□

Korollar D Sind $a_1, \dots, a_n, b \in \mathbb{Z}$ mit

$1 = ggT(a_1, b) = \dots = ggT(a_n, b)$, so gilt

$ggT(a_1 \cdots a_n, b) = 1$

Bew. mit Induktion nach n. Für $n = 0, 1$ ist nichts zu zeigen.

($n \to n+1$) $a_1, \dots a_n, a_{n+1}, b$

$$ggT(a_1 \cdots a_n, b) \overset{IV}{=} 1 = ggT(a_{n+1}, b)$$

Kor. 6

$$\Rightarrow ggT(a_1 \cdots a_{n+1}, b) = 1$$ □

11. Definition Eine Zahl $p \in \mathbb{N}$, $p \geq 2$ heißt Primzahl, wenn ± 1 und $\pm p$ die einzigen Teiler von p sind.
(1 ist also keine Primzahl).
Wir setzen $\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ ist Primzahl}\}$

Lemma Sei $n \in \mathbb{N}$ mit $n \geq 2$, setze

$$p(n) = \min \underbrace{\{k \in \mathbb{N} \mid k \mid n \text{ und } k \geq 2\}}_{\text{enthält } n \Rightarrow \text{nicht leer.}}$$

Dann $p(n) \in \mathbb{P}$.

Bew. Sei $d \geq 0$ ein Teiler von $p(n)$.
Es folgt $d \mid n$, also $d = 1$ oder $d \geq p(n)$
$\Rightarrow d = 1$ oder $d = p(n)$ □

#

Theorem (Euklid) Es gibt unendlich viele Primzahlen.

Beis Angenom, $\mathbb{P} = \{p_1 < p_2 < \dots < p_m\}$ wär endlich. Set $n = (p_1 \cdot p_2 \cdot \dots \cdot p_m) + 1$
$\Rightarrow n \geq 2$. Für $1 \leq j \leq m$ gilt $p_j \nmid n$
(denn sonst $p_j \mid 1$ ↯) $\Rightarrow p(n) \neq p_1, \dots, p_m$.
Ab $p(n) \in \mathbb{P}$ ↯ □

12. **Lemma** Si $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$.
Wenn gilt $p \mid a \cdot b$, so folgt $p \mid a$ oder $p \mid b$.

Beis Wenn $p \nmid a$ und $p \nmid b$, so folgt
$ggT(a,p) = 1 = ggT(b,p) \underset{\S 1.10.4}{\Longrightarrow} ggT(ab,p) = 1$
$\Rightarrow p \nmid ab$ □

13. Theorem (Hauptsatz der Arithmetik)

Sei $n \in \mathbb{N}$, $n \geq 2$. Dann existiert eindeutig bestimmt Primzahlen $p_1 \leq p_2 \leq \dots \leq p_s$ mit

$$n = p_1 \cdot p_2 \cdots \cdot p_s$$

Man nennt das die Primfaktorzerlegung von n, die p_j heißen Primfaktoren von n.

Beweis Existenz mit d. Induktionsprinzip.

Für $n = 0, 1$ wird nichts behauptet (v)

Sei jetzt $n \geq 2$, betrachte $p(n)$ wie in §1.11, schreibe $n = p(n) \cdot m$, $m < n$.

1. Fall $m = 1$ $\Rightarrow$ fertig, $n = p(n) \in \mathbb{P}$ (v)

2. Fall $m \geq 2$ $\Rightarrow$ es gibt $p_2 \leq \dots \leq p_s$

$m = p_2 \cdots p_s$ $\Rightarrow$ $n = p(n) \cdot p_2 \cdots p_s$ ist

$p(n) = p_1 \leq p_2$ fertig (v)

Eindeutigkeit mit d. Induktionsprinzip.

Für $n = 0, 1$ wird nichts behauptet (v)

Angenom. $n \geq 2$, $n = p_1 \cdots p_s = q_1 \cdots q_t$

mit Primzahl $p_1 \leq p_2 \leq \ldots \leq p_s$ $\quad s \geq 1$

$q_1 \leq q_2 \leq \quad \leq q_t$. $\quad t \geq 1$

Nach §1.12 gibt es ein $j \in \{1, \ldots, t\}$ mit

$p_1 \mid q_j \Rightarrow p_1 = q_j$ weil Primzahl.

Wenn $s = 1$, so folgt $t = 1$, weil $n = p_1$

Wenn $s \geq 2$, so folgt für $m = p_2 \cdots p_s$

$= q_1 \cdots q_{j-1} \cdot q_{j+1} \cdots q_t$ und $m < n$, dann

$s - 1 = t - 1$ und die Primfaktoren sind gleich

$s = t$ und die Primfaktoren von n sind eindeutig. □

Wir geben einen 2. Beweis für die Eindeutigkeit der Primfaktorzerlegung. Dazu wird eine Definition

Für $p \in \mathbb{P}$ und $z \in \mathbb{Z} - \{0\}$

$$\nu_p(z) = \max \underbrace{\{ l \in \mathbb{N} \mid p^l \mid z \}}_{\text{nicht leer, da } p^0 = 1 \mid z}$$

$|z|$ ist eine Schranke

$$\nu_p(0) = \infty$$

Man nennt $\nu_p(z)$ die p-adische Bewertung von z.

2. Beweis der Eindeutigkeit der Primfaktorzerlegung:

Schreibe $n = p_1 \cdots p_s$ $p_1 \leq \ldots \leq p_s$ Primzahl

Für $q \in \mathbb{P}$ sei l_q die Anzahl der $k \in \mathbb{N}$ mit $p_k = q$, $l_q = \#\{k \in \mathbb{N} \mid p_k = q\}$.

Es folgt $n = q^{l_q} \cdot m$, m Produkt der p_j mit $p_j \neq q$. Es folgt mit §1.10 Kor. D, dass $q \nmid m \Rightarrow \nu_q(n) = l_q$. Die linke Seite ist eindeutig von der gewählten Zerlegung $n = p_1 \cdots p_s$ □

Wir erhalten Folgt Variante des Hauptsatzes der Arithmetik.

14. Theorem (2. Form des Hauptsatzes der Arithmetik)

Sei $z \in \mathbb{Z}$ mit $z \neq 0$. Sei $\varepsilon(z) = \begin{cases} 1 & \text{wenn } z > 0 \\ -1 & \text{wenn } z < 0 \end{cases}$

Vorzeichenfunktion

Dann gilt

$$z = \varepsilon(z) \cdot \prod_{q \in \mathbb{P}} q^{\nu_q(z)}$$

Das Produkt auf der rechten Seite ist ein endliches Produkt, denn es gibt nur endlich viele $q \in \mathbb{P}$ mit $\nu_q(z) \geq 1$. Für die restlichen $q \in \mathbb{P}$ ist $\nu_q(z) = 0$, also gibt es im Produkt kein Beitrag. $\square$