Universität Konstanz
Fachbereich Mathematik und Statistik

BMA

(a) (i) Voraussetzung: $\forall a, b \in \mathbb{Z} : \exists c \in \mathbb{Z} : (b \mid a) \implies (a = b \cdot c)$
Behauptung: $\exists b \in \mathbb{Z} : \forall a \in \mathbb{Z} : b \mid a$:

Proof

zu zeigen $\exists b \in \mathbb{Z} : \forall a \in \mathbb{Z} : b \mid a$
setze $b := 1$, zu zeigen $b \in \mathbb{Z}$ und $\forall a \in \mathbb{Z} : b \mid a$.
Es gilt $b = 1 \in \mathbb{Z}$, noch zu zeigen:
$\forall a \in \mathbb{Z} : b \mid a$
sei ein $a \in \mathbb{Z}$ gegeben, zu zeigen $b \mid a$, d.h. zu zeigen $\exists c \in \mathbb{Z} : a = b \cdot c$:
Setze $c := a$, zu zeigen $c \in \mathbb{Z}$ und $a = b \cdot c$:
$c = a \in \mathbb{Z}$ gegeben
$b \cdot c = 1 \cdot a = a$ □

(ii) Voraussetzung: $\forall a, b \in \mathbb{Z} : \exists c \in \mathbb{Z} : (b \mid a) \implies (a = b \cdot c)$
Behauptung $\forall b \in \mathbb{Z} : \exists a \in \mathbb{Z} : b \mid a$

Proof

Zu zeigem $\forall b \in \mathbb{Z} : \exists a \in \mathbb{Z} : b \mid a$.
Sei ein $b \in \mathbb{Z}$ gegeben, zeige $\exists a \in \mathbb{Z} : b \mid a$
Setze $a := b$, zu zeigen $a \in \mathbb{Z}$ und $b \mid a$:
$a = b \in \mathbb{Z}$ gegeben
zu zeigen $b \mid a$, d.h. zu zeigen $\exists c \in \mathbb{Z} : a = b \cdot c$:
Setze $c := 1$, zu zeigen $c \in \mathbb{Z}$ und $a = b \cdot c$
$c = 1 \in \mathbb{Z}$ gegeben
$b \cdot c = b \cdot 1 = b = a$ □

(b) Voraussetzung: $\forall a, b \in \mathbb{Z} : \exists c \in \mathbb{Z} : (b \mid a) \implies (a = b \cdot c)$
Behauptung: $\forall n \in \mathbb{N} : \forall a \in \mathbb{Z} : \{b \in \mathbb{Z} : n \mid (a - b)\} = \{a + k \cdot n : k \in \mathbb{Z}\}$

Proof

Zu zeigen $\forall n \in \mathbb{N} : \forall a \in \mathbb{Z} : \{b \in \mathbb{Z} : n \mid (a - b)\} = \{a + k \cdot n : k \in \mathbb{Z}\}$
Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ gegeben, zu zeigen:

$$\{b \in \mathbb{Z} : n \mid (a - b)\} = \{a + k \cdot n : k \in \mathbb{Z}\},$$

also zu zeigen

$$\{b \in \mathbb{Z} : n \mid (a - b)\} \subseteq \{a + k \cdot n : k \in \mathbb{Z}\} \text{ und}$$

$$\{b \in \mathbb{Z} : n \mid (a - b)\} \supseteq \{a + k \cdot n : k \in \mathbb{Z}\}$$

"$\subseteq$":
Sei ein x in $\{b \in \mathbb{Z} : n \mid (a - b)\}$ gegeben, zu zeigen x in $\{a + k \cdot n : k \in \mathbb{Z}\}$
Also $x \in \mathbb{Z}$ und $n \mid (a - x)$ gegeben, zu zeigen $a + k \cdot n = x$ und $k \in \mathbb{Z}$.

Da $n \mid (a-x)$, existiert ein Objekt c für das gilt $(a-x) = n \cdot c$.
Setze $k = -c$, zu zeigen $k \in \mathbb{Z}$ und $x = a + k \cdot n$
$k = -c \in \mathbb{Z}$ gegeben
$a + k \cdot n = a + (-c) \cdot n = a - c \cdot n = x$, was zu zeigen war

"$\supseteq$":
Sei ein x in $\{a + k \cdot n : k \in \mathbb{Z}\}$ gegeben, zu zeigen x in $\{b \in \mathbb{Z} : n \mid (a-b)\}$
Es gilt $x = a + k \cdot n$ für $k \in \mathbb{Z}$, zu zeigen $x \in \mathbb{Z}$ und $n \mid (a-x)$.
Da $n \in \mathbb{N} \subset \mathbb{Z}$ gegeben, ist $a, n, k \in \mathbb{Z}$ gegeben, folgt $x = a + k \cdot n \in \mathbb{Z}$ gegeben.
Zu zeigen $n \mid (a-x)$, d.h. zu zeigen $\exists c \in \mathbb{Z} : a - x = n \cdot c$. Setze $c \coloneqq -k$, zu zeigen $c \in \mathbb{Z}$ und $a - x = n \cdot c$:
$c = -k \in \mathbb{Z}$ gegeben
$n \cdot c \overset{\text{Def.}}{=} n \cdot (-k) = -n \cdot k = 0 - n \cdot k = (a-a) - n \cdot k = a - (a + n \cdot k) \overset{\text{Def.}}{=} a - x$ $\square$