Satz und Def. (Division mit Rest):

Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$.

Dann ex. eindeutig bestimmte $q, r \in \mathbb{Z}$ mit:

$a = q \cdot n + r \quad , \quad 0 \leq r < n.$

Man def.: $\text{Rest}_n(a) := r.$

Bsp.:

$\underset{a}{7} = \underset{q}{2} \cdot \underset{n}{3} + \underset{r}{1} \quad , \quad 0 \leq r < 3$

$\underset{a}{12} = \underset{q}{3} \cdot \underset{n}{4} + \underset{r}{0} \quad , \quad 0 \leq r < 4$

$\underset{a}{-5} = \underset{q}{-3} \cdot \underset{n}{2} + \underset{r}{1} \quad , \quad 0 \leq r < 2$

$\underset{a}{2} = \underset{q}{0} \cdot \underset{n}{3} + \underset{r}{2} \quad , \quad 0 \leq r < 3$

Def.:

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

$a \mid b :\Leftrightarrow \exists\, c \in \mathbb{Z} : a \cdot c = b.$

(a teilt b)

Bsp.:

$3 \mid 6$, denn $\underset{a}{3} \cdot \underset{c}{2} = \underset{b}{6}$

Satz:

Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$.

Dann gilt:

$\text{Rest}_n(a) = \text{Rest}_n(b) \Leftrightarrow n \mid (b - a)$

Bew.:

Schreibe $a = q_1 \cdot n + r_1$, $b = q_2 \cdot n + r_2$

mit $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ und $0 \leq r_1, r_2 < n$.

Es ist $\text{Rest}_n(a) = r_1$, $\text{Rest}_n(b) = r_2$

„$\Rightarrow$" Es gelte: $\text{Rest}_n(a) = \text{Rest}_n(b)$, d.h. $r_1 = r_2$.

$\Rightarrow b - a = (q_2 \cdot n + r_2) - (q_1 \cdot n + r_1) = \underbrace{(q_2 - q_1)}_{\in \mathbb{Z}} \cdot n$

$\Rightarrow n \mid (b - a)$

„$\Leftarrow$" Es gelte: $n \mid (b - a)$

$\Rightarrow \exists\, c \in \mathbb{Z}: \quad n \cdot c = b - a$

$\Rightarrow a = b - n \cdot c = q_2 \cdot n + r_2 - n \cdot c = \underbrace{(q_2 - c)}_{\in \mathbb{Z}} \cdot n + r_2$

(Eind.)

$\Rightarrow r_1 = r_2$, d.h. $\text{Rest}_n(a) = \text{Rest}_n(b)$. □.

Satz und Def.:

Sei $n \in \mathbb{N}$.

Wir def.: $\forall a, b \in \mathbb{Z}: \; a \sim b :\Leftrightarrow n \mid (b - a)$

Dann gilt:

$\sim$ ist eine Äqui-Rel. auf $\mathbb{Z}$.

Bew.:

Seien $a, b, c \in \mathbb{Z}$.

(i) $a \sim a \Leftrightarrow n \mid (a - a) \Leftrightarrow n \mid 0$ (w) ✓

(ii) $a \sim b \Rightarrow n \mid (b - a) \Rightarrow \exists\, c \in \mathbb{Z}: n \cdot c = b - a$

$\Rightarrow n \cdot \underbrace{(-c)}_{\in \mathbb{Z}} = a - b \Rightarrow n \mid (a - b)$

$\Rightarrow b \sim a$.

(iii) $a \sim b \wedge b \sim c$

$\Rightarrow n \mid (b-a) \wedge n \mid (c-b)$

$\Rightarrow \exists d_1, d_2 \in \mathbb{Z}: \; n \cdot d_1 = b-a \wedge n \cdot d_2 = c-b$

$\Rightarrow n \cdot \underbrace{(d_1 + d_2)}_{\in \mathbb{Z}} = n \cdot d_1 + n \cdot d_2 = (b-a) + (c-b) = c-a$

$\Rightarrow n \mid (c-a)$

$\Rightarrow a \sim c.$ □.

Def.:

Sei $n \in \mathbb{N}$.

(i) $\forall a \in \mathbb{Z}: \; \bar{a} := [a] = \{ b \in \mathbb{Z} \mid a \sim b \}$.

(ii) $\mathbb{Z}/n\mathbb{Z} := \{ \bar{a} \mid a \in \mathbb{Z} \}$

Bem.:

(i) $\bar{a} = \{ b \in \mathbb{Z} \mid a \sim b \} = \{ b \in \mathbb{Z} \mid n \mid (b-a) \}$

$= \{ b \in \mathbb{Z} \mid \exists c \in \mathbb{Z}: \; n \cdot c = b-a \}$

$= \{ b \in \mathbb{Z} \mid \exists c \in \mathbb{Z}: \; b = a + n \cdot c \}$

$= \{ a + n \cdot c \mid c \in \mathbb{Z} \}$

$= a + n \cdot \mathbb{Z}.$

(ii) $\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \ldots, \overline{n-1} \}$

Bew.:

„$\geq$" klar.

„$\leq$" Sei $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ mit $a \in \mathbb{Z}$

Schreibe $a = q \cdot n + r$ mit $q, r \in \mathbb{Z}$, $0 \leq r < n$.

$\Rightarrow n \cdot q = a - r \Rightarrow n \mid (a-r)$

$\Rightarrow a \sim r \Rightarrow \bar{a} = \bar{r} \in \{ \bar{0}, \bar{1}, \ldots, \overline{n-1} \}$. □.

Def.:

(i) $\forall \bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}: \quad \bar{a} + \bar{b} := \overline{a+b}$

(ii) $\forall \bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}: \quad \bar{a} \cdot \bar{b} := \overline{a \cdot b}$

Satz:

(i) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring.

(ii) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist ein Körper $\Leftrightarrow$ n ist eine Primzahl.

Def.:

Sei p eine Primzahl. $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Satz:

Für alle $a, p \in \mathbb{Z}$, $n \in \mathbb{N}$ gilt:

$\bar{a} = \overline{a + q \cdot n}$ Bzw $a = a + q \cdot n$ in $\mathbb{Z}/n\mathbb{Z}$

Bew.:

$\bar{a} = \overline{a + q \cdot n} \quad \Leftrightarrow \quad a \sim a + q \cdot n$

$\Leftrightarrow \quad n \mid (a + qn) - a$

$\Leftrightarrow \quad n \mid q \cdot n \quad (\omega).$

□

Rechnen in $\mathbb{Z}/n\mathbb{Z}$:

Es gilt stets: $\forall a \in \mathbb{Z}/n\mathbb{Z}: \quad a = a + q \cdot n \quad \forall q \in \mathbb{Z}$

Bsp.:

(1) $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$

$1 + 2 = 3$

$2 + 2 = 4 = 4 - 1 \cdot 4 = 0$

$2 + 3 = 5 = 5 - 1 \cdot 4 = 1$

$17 \cdot 25 = (17 - 4 \cdot 4) \cdot (25 - 7 \cdot 4) = 1 \cdot 1 = 1$

(2) $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$ ist ein Körper:

$1 \cdot 1 = 1 \Rightarrow 1^{-1} = 1$

$2 \cdot 2 = 4 = 4 - 1 \cdot 3 = 1 \Rightarrow 2^{-1} = 2$

$\Rightarrow \forall x \in \mathbb{F}_3 \setminus \{0\} \; \exists y \in \mathbb{F}_3 : x \cdot y = 1$ (jedes Element $\neq 0$ hat ein multiplikatives Inverses)

(3) $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ ist ein Körper:

$1 \cdot 1 = 1 \Rightarrow 1^{-1} = 1$

$2 \cdot 3 = 6 = 6 - 1 \cdot 5 = 1 \Rightarrow 2^{-1} = 3$

$3 \cdot 2 = 6 = 6 - 1 \cdot 5 = 1 \Rightarrow 3^{-1} = 2$

$4 \cdot 4 = 16 = 16 - 3 \cdot 5 = 1 \Rightarrow 4^{-1} = 4$

$\Rightarrow \forall x \in \mathbb{F}_5 \setminus \{0\} \; \exists y \in \mathbb{F}_5 : x \cdot y = 1$ (jedes Element $\neq 0$ hat ein multiplikatives Inverses)

$4 \cdot 0 = 0$

$4 \cdot 1 = 4$

$4 \cdot 2 = 8 = 3$

$4 \cdot 3 = 12 = 2$

$4 \cdot 4 = 16 = 1$ ✓

(4) $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ ist kein Körper:

$1 \cdot 2 = 2 \neq 1$

$2 \cdot 2 = 4 = 0 \neq 1$

$2 \cdot 3 = 6 = 2 \neq 1$

$\Rightarrow 2 \in \mathbb{Z}/4\mathbb{Z}$ hat kein multiplikatives Inverses.