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.:

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

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

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

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

Def.:

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

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

(a teilt b)

Bsp.:

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

Satz:

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

Dann gilt:

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

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 $\mathrm{Rest}_n(a) = r_1$, $\mathrm{Rest}_n(b) = r_2$

„$\Rightarrow$" Es gelte: $\mathrm{Rest}_n(a) = \mathrm{Rest}_n(b)$, 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: $n \mid (b - a)$

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

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

$\overset{\text{(Eind.)}}{\Rightarrow} r_1 = r_2$, d.h. $\mathrm{Rest}_n(a) = \mathrm{Rest}_n(b)$. $\square$.

Satz und Def.:

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

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

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

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

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

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

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

$\Rightarrow a \sim c.$ $\square$.

Def.:

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

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

(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.:

„$\supseteq$" klar.

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

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

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

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

Def.:

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

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

$+ , \cdot$ sind wohldef.

Seien $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}/n\mathbb{Z}$ und gelte:

$\bar{a} = \bar{c} \quad , \bar{b} = \bar{d}$

z.z: (i) $\overline{a+b} = \overline{c+d}$

(ii) $\overline{a \cdot b} = \bar{c} \cdot \bar{d}$.

$\bar{a} = \bar{c}$ und $\bar{b} = \bar{d}$

$\Rightarrow a \sim c$ und $b \sim d$

$\Rightarrow n \mid (c-a)$ und $n \mid (d-b) \quad (*)$

(i) $\overset{(*)}{\Rightarrow} n \mid ((c-a) + (d-b))$

$\Rightarrow n \mid ((c+d) - (a+b))$

$\Rightarrow a+b \sim c+d$

$\Rightarrow \overline{a+b} = \overline{c+d} \quad \Rightarrow$ (i)

(ii) $\overset{(*)}{\Rightarrow} n \mid b \cdot (c-a)$ und $n \mid c \cdot (d-b)$

$\Rightarrow n \mid (b \cdot (c-a) + c \cdot (d-b))$

$\Rightarrow n \mid (b \cdot c - ab + cd - cb)$

$\Rightarrow n \mid (cd - ab)$

$\Rightarrow ab \sim cd$

$\Rightarrow \overline{a \cdot b} = \overline{c \cdot d}$. $\square$.

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

z.z.: $(\mathbb{F}_p, +, \cdot)$ ist ein Körper.

Bew.:

(i) Für alle $\bar{a}, \bar{b}, \bar{c} \in \mathbb{F}_p$ gilt:

$$(\bar{a} + \bar{b}) + \bar{c} = \overline{(a+b)} + \bar{c} = \overline{(a+b)+c} = \overline{a+(b+c)}$$
$$= \bar{a} + \overline{(b+c)} = \bar{a} + (\bar{b} + \bar{c})$$

(ii) Für alle $\bar{a} \in \mathbb{F}_p$ gilt:

$$\bar{a} + \bar{0} = \overline{a+0} = \bar{a} = \overline{0+a} = \bar{0} + \bar{a}$$

d.h. $\bar{0}$ ist das neutrale Element bzgl $+$

(iii) Für alle $\bar{a} \in \mathbb{F}_p$ gilt:

$$\bar{a} + \overline{(-a)} = \overline{a + (-a)} = \bar{0} = \overline{(-a)+a} = \overline{(-a)} + \bar{a}$$

d.h.: $\overline{(-a)}$ ist das additive Inverse zu $\bar{a}$ bzgl $+$.

(iv) Für alle $\bar{a}, \bar{b} \in \mathbb{F}$ gilt:

$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$$

(i) - (iv) $\Rightarrow$ $(\mathbb{F}_p, +)$ ist eine kommutative Gruppe.

(v) Für alle $\bar{a}, \bar{b}, \bar{c} \in \mathbb{F}_p$ gilt:

$$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{(a \cdot b)} \cdot \bar{c} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot (b \cdot c)}$$
$$= \bar{a} \cdot \overline{(b \cdot c)} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$$

(vi) Für alle $\bar{a} \in \mathbb{F}_p$ gilt:

$$\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a} = \overline{1 \cdot a} = \bar{1} \cdot \bar{a}$$

d.h. $\bar{1}$ ist das neutrale Element bzgl $\cdot$

(vii) Sei $\bar{a} \in \mathbb{F}_p \setminus \{\bar{0}\}$.

Schreibe $\bar{a} = \bar{b}$ mit $b \in \{1, \dots, p-1\}$.

Da p eine Primzahl ist, gilt: $\operatorname{ggT}(b, p) = 1$.

Also gibt es $c, d \in \mathbb{Z}$ mit $c \cdot b + d \cdot p = 1$

$\Rightarrow \bar{c} \cdot \bar{b} + \bar{d} \cdot \underbrace{\bar{p}}_{=\bar{0}} = \bar{1} = \bar{b} \cdot \bar{c} + \bar{d} \cdot \underbrace{\bar{p}}_{=\bar{0}}$

$\Rightarrow \bar{c} \cdot \bar{b} = \bar{1} = \bar{b} \cdot \bar{c} \quad \Rightarrow \bar{c} \cdot \bar{a} = \bar{1} = \bar{a} \cdot \bar{c}$

$\Rightarrow \bar{c}$ ist das multiplikative Inverse zu $\bar{a}$ bzgl. $\cdot$

Alternativ:

Def.: $f : \mathbb{F}_p \to \mathbb{F}_p$, $f(\bar{x}) = \bar{a} \cdot \bar{x}$.

f ist injektiv:

Seien $\bar{x_1}, \bar{x_2} \in \mathbb{F}_p$ und gelte $f(\bar{x_1}) = f(\bar{x_2})$

$\Rightarrow \bar{a}\, \bar{x_1} = \bar{a} \cdot \bar{x_2} \quad \Rightarrow \bar{a} \cdot (\bar{x_1} - \bar{x_2}) = \bar{0}$

$\Rightarrow \overline{a \cdot (x_1 - x_2)} = \bar{0} \quad \Rightarrow p \mid a \cdot (x_1 - x_2)$

p ist eine Primzahl $\Rightarrow p \mid a \vee p \mid (x_1 - x_2)$

$\Rightarrow \bar{a} = \bar{0} \vee \overline{x_1 - x_2} = \bar{0}$

$\overset{\bar{a} \neq \bar{0}}{\Rightarrow} \overline{x_1 - x_2} = 0 \quad \Rightarrow \overline{x_1} - \overline{x_2} = 0 \quad \Rightarrow \overline{x_1} = \overline{x_2}$.

Da $|\mathbb{F}_p| = p < \infty$ folgt: f ist bijektiv

$\Rightarrow \exists\, \bar{c} \in \mathbb{F}_p : f(\bar{c}) = \bar{1} \quad \Rightarrow \bar{a} \cdot \bar{c} = \bar{1}$.

(viii) Für alle $\bar{a}, \bar{b} \in \mathbb{F}_p$ gilt:

$\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \cdot \bar{a}$.

(ix) Für alle $\bar{a}, \bar{b}, \bar{c} \in \mathbb{F}_p$ gilt:

$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \overline{b + c} = \overline{a \cdot (b + c)}$

$= \overline{a \cdot b + a \cdot c} = \overline{a \cdot b} + \overline{a \cdot c}$

$= \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$.

(i) - (ix) $\Rightarrow (\mathbb{F}_p, +, \cdot)$ ist ein Körper. $\square$.