Restklassen

Fragen?

$R_m = \mathbb{Z}_m$? z.B. $R_5 = \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \cancel{\bar{5}}, \cancel{\bar{6}}, \dots\}$

$\bar{5} = \bar{0}$, $\bar{6} = \bar{1}$

$\bar{0} = \{0, 5, 10, 15, \dots\}$, $\bar{1} = \{1, 6, 11, 16, \dots\}$, ..., $\bar{4} = \{4, 9, 14, 19, \dots\}$, $\bar{5} = \{5, 10, 15, \dots\}$

Repräsentant von $\bar{4} = \{\dots, 4, 9, 14, 19, \dots\}$? z.B. 14 ist ein Repräsentant von $\bar{4}$.

da $14 \in \bar{4}$.

$\bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} \cup \bar{4} = \mathbb{Z}$.

$\subseteq$: klar!

$\supseteq$: Sei $z \in \mathbb{Z}$. Sei $r = z \bmod 5$ ($0 \le r < 5$), d.h. $r \equiv z \pmod 5$

d.h. $z \in \bar{r}$. mit $0 \le r < 5$

$2^{980} \bmod 243$?

$$(\underbrace{2^2}_{4})^{490} = (\underbrace{4^2}_{16})^{245} = 16 \cdot (\underbrace{16^2}_{256 \,\equiv\, 13})^{122} = 16 \cdot (\underbrace{13^2}_{169})^{61} = 16 \cdot 169 \cdot (\underbrace{169^2}_{\equiv\, 130})^{30}$$

$$= 16 \cdot 169 \cdot (\underbrace{130^2}_{\equiv\, 133})^{15} = 16 \cdot 169 \cdot 133 \cdot (\underbrace{133^2}_{\equiv\, 193})^{7} =$$

$$= 16 \cdot 169 \cdot 133 \cdot 193 \cdot (193^2)^3 = \dots$$

* **Restklassen.** Was sind die Restklassen von $\mathbb{Z}_3, \mathbb{Z}_4$?

Lösung.

Menge von Mengen!

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}, \cancel{\bar{3}}, \cancel{\bar{4}}, \cancel{\ldots}\}$$

$$\bar{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 3\} = 0 + 3\cdot\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

$$\bar{1} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 3\} = 1 + 3\cdot\mathbb{Z} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$

$$\bar{2} = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 3\} = 2 + 3\cdot\mathbb{Z} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

$$\bar{3} = \ldots\ldots = \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\}$$

$$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

$$\bar{0} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$

$$\bar{1} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$

$$\bar{2} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$

$$\bar{3} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

Eigener Lösungsversuch.

Verknüpfungstafeln. Bilden Sie die Verknüpfungstafeln bzgl. $+/\cdot$ von $\mathbb{Z}_3$ & $\mathbb{Z}_4$.

Lösung.

$\bar{1}+\bar{2} \overset{\text{Def.}}{=} \overline{1+2} = \bar{3} \overset{\text{s.o.}}{=} \bar{0}$

Gleichheit von Mengen!

$\mathbb{Z}_3$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\boxed{\bar{3}=\bar{0}}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{4}=\bar{1}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\boxed{\bar{4}=\bar{1}}$

$\bar{2}\cdot\bar{2} \overset{\text{Def.}}{=} \overline{2\cdot 2} = \bar{4} = \bar{1}$

$\mathbb{Z}_4$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}=\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{5}=\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{6}=\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}=\bar{0}$	$\bar{6}=\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{9}=\bar{1}$

Eigener Lösungsversuch.

Zusammenhang von "≡" und "=" bei Zahlen und Restklassen. Die Zahlen 5 und 13 sind natürlich nicht gleich, aber es gelten folgende äquivalente Aussagen:

- **Zahlen "=":** $5 = 13 + q \cdot 8$ für ein $q \in \mathbb{Z}$ (gleich bis auf ein Vielfaches von 8)
- **Zahlen "≡":** $5 \equiv 13 \pmod{8}$
- **Restklassen "=":** $\overline{5} = \overline{13}$ in $\mathbb{Z}_8$

Gleichheit von Mengen!

Rechnen mit Restklassen. Berechnen Sie in $\mathbb{Z}_{10}$ ohne Taschenrechner:

$5134 \equiv 4 \pmod{10}$

$$\overline{5134}\cdot\overline{21}+\overline{235}\cdot\overline{24}-\overline{338}\cdot\overline{446} = \overline{4}-\overline{8} = \overline{-4} = \overline{6}$$

Lösung.

$$\underbrace{\underbrace{\overline{4}\cdot\overline{1}}_{\overline{4}} + \underbrace{\overline{5}\cdot\overline{4}}_{\overline{20}=\overline{0}}}_{\overline{4}} - \underbrace{\overline{8}\cdot\overline{6}}_{\overline{48}=\overline{8}}$$

$-4 \equiv 6 \pmod{10}$

Eigener Lösungsversuch.

Lineare Gleichung, Teil 1. Bestimmen Sie alle $\overline{x} \in \mathbb{Z}_{12}$ mit $\overline{4} \cdot \overline{x} + \overline{2} = \overline{1}$.

Lösung.

Zusammenfassung s.o.

$$\overline{4}\,\overline{x} + \overline{2} = \overline{1} \overset{-\overline{2}}{\Longrightarrow} \underbrace{\overline{4}\,\overline{x}}_{\overline{4x}} = \underbrace{\overline{-1}}_{\overline{11}}, \text{ also } \overline{4x} = \overline{11} \Longleftrightarrow 4x = 11 + q \cdot 12$$

$$\Longleftrightarrow \underbrace{4x + 12 \cdot \underbrace{(-q)}_{y} = 11}_{\text{diophantische Gleichung!}}$$

<u>Lösbar?</u> $\operatorname{ggT}(4,12) = 4 \nmid 11$, d.h. <u>nicht</u> lösbar

d.h. es gibt kein $\overline{x} \in \mathbb{Z}_{12}$ als Lösung!

Eigener Lösungsversuch.

Lineare Gleichung, Teil 2. Bestimmen Sie alle $\overline{x} \in \mathbb{Z}_{1024}$ mit

1. $\overline{5} \cdot \overline{x} = \overline{1}$
2. $\overline{2} \cdot \overline{x} = \overline{4}$

Lösung. 1. $\overline{5\cdot x} = \overline{1} \iff 5x = 1 + q \cdot 1024 \quad (q \in \mathbb{Z}) \iff \overbrace{5x + 1024\underbrace{(-q)}_{y} = 1}^{\text{dioph. Gl.}}$

Lösbar? $\operatorname{ggT}(5, \underbrace{1024}_{2^{10}}) = \underline{1} \mid 1$ ✓.

(1.) EEA

$a_i = q_i\, b_i + r_i$	x_i	y_i	$\operatorname{ggT}(a,b) = a_i\, x_i + b_i\, y_i$
$5 = 0 \cdot 1024 + 5$	$\boxed{205}$		$1 =$
$1024 = 204 \cdot 5 + 4$	-1	205	$1 = 1024\,(-1) + 5 \cdot 205$
$5 = 1 \cdot 4 + \boxed{1}$	1	-1	$1 = 5 \cdot 1 + 4 \cdot (-1)$
$4 = 4 \cdot \boxed{1} + 0$	0	1	$1 = 4 \cdot 0 + 1 \cdot 1$

ggT

$x_0 = 205$

(2.) ✗

Zusammenfassung!

(3.) Allg. Lsg: $x = 205 + z \cdot \frac{1024}{1} = 205 + z \cdot 1024 \iff \overline{x} = \overline{205}$

d.h. $\overline{x} = \overline{205}$ ist eindeutige Lösung! [Probe: $\overline{5} \cdot \overline{205} = \overline{1025} = \overline{1}$ ✓]

2. $\overline{2} \cdot \overline{x} = \overline{4} \iff \overline{2x} = \overline{4} \iff 2x = 4 + k\, 1024 \iff \underbrace{2x + 1024\underbrace{(-k)}_{y} = 4}_{\text{dioph. Gl.}}$

Lösbar? $\operatorname{ggT}(2, 1024) = 2 \mid 4$ ✓

(1.) EEA:

$a = q\, b + r$	x	y	$\operatorname{ggT} = ax + by$
$2 = 0 \cdot 1024 + \boxed{2}$	$\boxed{1}$	0	$2 = 2 \cdot 1 + 1024 \cdot 0$
$1024 = 2^9 \cdot \boxed{2} + 0$	0	1	$2 = 1024 \cdot 0 + 2 \cdot 1$

$x_0 = 1$

Hier direkt durch Hinsehen:

$\overline{2} \cdot \overline{x} = \overline{4}$

$\Rightarrow \overline{x} = \overline{2}$

(2.) Lösung von $2x + 1024y = 4$ $\quad \cdot 2 \quad x_0 = 2 \cdot 1 = 2$

(3.) Allg. Lsg: $x = 2 + z\,\frac{1024}{2} = 2 + z \cdot 512 = \quad \ldots, -510, 2, 514, 1026, \ldots$

Restklassen dazu: $\overline{x} = \overline{2} + \underbrace{\overline{z \cdot 512}}_{\left\{\begin{array}{ll}\overline{0} & z \text{ gerade} \\ \overline{512} & z \text{ ungerade}\end{array}\right.} = \ldots, \underset{\overline{514}}{\overset{\shortparallel}{\overline{-510}}}, \overline{2}, \overline{514}, \underset{\overline{2}}{\overset{\shortparallel}{\overline{1026}}}, \ldots$

Wir bekommen <u>zwei</u> Lösungen $\overline{x} = \overline{2}, \overline{514} \in \mathbb{Z}_{1024}$ [Probe: $\overline{2} \cdot \overline{2} = \overline{4}$ ✓, $\overline{2} \cdot \overline{514} = \overline{1028} = \overline{4}$ ✓]

Eigener Lösungsversuch.