Kongruenzklasse $C(a) := \{n \mid n \equiv a \bmod m\}$ (zum Modul m)

$C(a) = C(b) \;\vee\; C(a) \cap C(b) = \varnothing$ *(Kongruenz!)*

ferner $C(a) = C(b) \;\leftrightarrow\; a \in C(b)$

$r \in C(a)$ r Repräsentant von $C(a)$

$\overline{a} := C(a)$ *(Schreibweise)*

$0, 1, \cdots, m-1$ vollständiges Repräsentantensystem

$\overline{0}, \overline{1}, \cdots, \overline{m-1}$ Partition *(Klasseneinteilung)*

(allgemein) (vollständiges System von) Restklassen $\bmod m$

r_i $(0 \leq i \leq m-1)$ vollständiges System von Repräsentanten

$\Leftrightarrow$ $\mathbb{Z}_m := \{C(i) \mid (0 \leq i \leq m-1)\}$ Partition von $\mathbb{Z}$

$(\mathbb{Z}_m, \oplus, \odot)$ ($\mathbb{Z}_m$ Ring)

(Addition) $C(a) \oplus C(b) =: C(a+b)$ $\overline{a} + \overline{b} = \overline{a+b}$

(Multiplikation) $C(a) \odot C(b) =: C(ab)$ $\overline{a} \cdot \overline{b} = \overline{a}\,\overline{b} = \overline{ab}$

(denn:) $\equiv$ Kongruenzrelation $\Rightarrow$ *„wohldefiniert“*

$\overline{a} \oplus \overline{0} = \overline{a}$ $\overline{0}$ Nullelement

$\overline{1} \odot \overline{a} = \overline{a}$ $\overline{1}$ Einselement

$\overline{a} \oplus \overline{m-a} = \overline{0}$ negatives *(entgegengesetztes)* Element

$ab = m \;\Rightarrow\; \overline{a}\overline{b} = \overline{0}$ a, b Nullteiler *(wenn a, b echte Teiler)*

$(r, m) = 1$ r und m relativ prim

dann: $\overline{r}$ $\overline{r}$ prime Restklasse

$\Leftrightarrow$ $(\exists r')\; \overline{r} \odot \overline{r'} = \overline{1}$ $\overline{r}$ invertierbar (Einheit)

denn: $\Leftrightarrow\; 1 = \lambda r + \mu m$ $\overline{r'} = \overline{\lambda} =: \overline{r}^{-1}$

(prime Restklassen(-gruppe))

Die Einheiten in $\mathbb{Z}_m$ sind (genau) die primen Restklassen.

(daher:) Ist m prim, so sind alle Klassen außer $\overline{0}$ Einheiten.

$\mathbb{Z}_m$ nullteilerfrei $\Leftrightarrow$ m prim. ($\mathbb{Z}_p$ (p prim) ist Körper.)