**Satz von der Division mit Rest:**(s.o.)

$\forall m \in N, b \in N_0 \quad \exists_{\text{eindeutig}}\ q, r \in N_0 : \quad b = q \cdot m + r \quad mit\ 0 \le r < m$

Definition der Kongruenz von a und b modulo m.

$\forall m \in N, \quad a, b \in N_0 : a \underset{m}{\equiv} b \Leftrightarrow m \mid (a-b) \Leftrightarrow \exists\, k \in Z : m \cdot k = a - b$

Man schreibt dann $a = b \mod m$ oder $a \underset{m}{\equiv} b$ lies: $a = b$ modulo $m$

In obigem Satz gilt $q \cdot m = b - r \quad mit\ 0 \le r < m$, also gilt:

$b = r \mod m$ oder $b \underset{m}{\equiv} r$ lies: $b = r$ modulo $m$ d.h. Jede Zahl ist kongruent zu ihrem Rest modulo m.

Satz: $a \underset{m}{\equiv} b \Leftrightarrow \left( a \underset{m}{\equiv} r \ \wedge \ b \underset{m}{\equiv} r \right)$ d.h. a und b sind kongruent modulo m genau dann, wenn sie beim Teilen durch m denselben nicht-negeativen Rest lassen.

Bew.: $" \Rightarrow "_{o.B.d.A}\ a > b \quad a \underset{m}{\equiv} b \Rightarrow m \cdot k = a - b \Rightarrow a = k \cdot m + b$. Für b existiert eine Darstellung mit Rest $b = q \cdot m + r \quad mit\ 0 \le r < m$, also bleibt zu zeigen, dass a auch diesen Rest hat: $a = k \cdot m + b = k \cdot m + q \cdot m + r = (k+q) \cdot m + r \quad mit\ 0 \le r < m$ q.e.d ($" \Rightarrow "$)

Bew.: $" \Leftarrow "_{o.B.d.A.}\ a > b \quad \left( a \underset{m}{\equiv} r \ \wedge \ b \underset{m}{\equiv} r \right) \Rightarrow a = k \cdot m + r \ \wedge b = q \cdot m + r \Rightarrow$

$\Rightarrow a - b = (k-q) \cdot m \Rightarrow a \underset{m}{\equiv} b$ mit natürlichen Zahlen k und q. q.e.d ($" \Leftarrow "$) q.e.d.

Bemerkung: In der Schule nimmt man diesen Satz als Definition und macht alle Zusammenhänge an Beispielen, an Strecken und an Bündelungen klar.
Durch diesen Satz wird offensichtlich, dass die Kongruenz modulo m ein Äquivalenzrelation ist (reflexiv, symmetrisch, transitiv), die zugehörigen Klassen heißen Restklassen modulo m.

In der **Zahlentheorie** ist es üblich, die Klasse von $a$ mit $\bar{a}$ zu bezeichnen.
Bevorzugter Repräsentant der Klasse ist der nicht-negative Rest r, denn alle Elemente gemeinsam haben, $\bar{a} = \bar{r}$.
In der funktionalen Sicht betrachtet man die Funktion
$\mathbf{Mod} : \ Z \to Z_m := \{0, 1, ...., m-1\}$, die jeder ganzen Zahl ihren Rest modulo m zuordnet. $\mathbf{Mod}(a, m) := r \quad mit \quad a = r \mod m \ \wedge 0 \le r < m$
Diese Sicht passt zur Beschaffung der Reste mit Computerwerkzeugen:
Mathematica: Mod(27,5) ergibt 2 // TI, Derive, GTR mod(27,5)
MuPad modp(27,6) Das p steht für "positiv", dort auch mods(28,6) ergibt -2.
In mehreren Werkzeugen ist außer der funktionalen Schreibweise mit vorn stehendem Funktionssymbol (Präfix-Schreibweise) auch die Infix-Schreibweise möglich: Maple, MuPAD 27 mod 5, Mathematica 27 ~Mod~ 5,
Dabei steht der Operator zwischen den Operanden.
In algebraischer Sicht betrachtet man $Z_m := \{0, 1, ...., m-1\}$ einfach als eine Menge, für die es nun gilt Verknüpfungen zu definieren.