

23. Homomorphieregel

für alle $a, b \in \mathbb{Z}$:

$$(a + b)_{\text{mod } n} = (a \text{ mod } n) +_{\text{mod } n} (b \text{ mod } n)$$

$$(a \cdot b)_{\text{mod } n} = (a \text{ mod } n) \cdot_{\text{mod } n} (b \text{ mod } n)$$

Schreibweise:

$$a \text{ mod } n = r \leftrightarrow a \equiv r \text{ (mod } n)$$