

## 21. Rechnen modulo 2

allgemein: Rechnen modulo n

$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  (Restklassen modulo n)

Für  $a, b \in \mathbb{Z}_n$ , definiere:

- $a +_{\text{mod } n} b := (a + b) \text{ mod } n \in \mathbb{Z}_n$
- $a \cdot_{\text{mod } n} b := (a \cdot b) \text{ mod } n$
- $a -_{\text{mod } n} b := (a - b) \text{ mod } n$

allgemein: Rechnen modulo 2

$+_{\text{mod } n}$	0	1
0	0	1
1	1	0

$-_{\text{mod } n}$	0	1
0	0	1
1	1	0

$\cdot_{\text{mod } n}$	0	1
0	0	0
1	0	1