

PROGRAMMING LOGIC AND TECHNIQUES

Modulo operator

Modulo

□ When is $13 + 5 = 0$?

□ When is $12 + 7 = 7$?

□ When is $1 + 7 = 1$?

Modulo

- The **modulo** operator is a binary operator that looks for the remainder of a division, called the **modulus**.
- Therefore, the notation $a \pmod b = r$ means that r is the remainder of the division of the dividend a by the divisor b

Modulo

□ *Example:* $13 \pmod{2} = 1$

□ *Example:* $13 \pmod{7} = 6$

Modulo

- The operation $(\text{mod } 2)$ is oftentimes used to check if a number is even or odd.
- However, this is not the only use of modulo.
Time-keeping is simultaneously calculated $(\text{mod } 24)$ and $(\text{mod } 7)$

Modulo

- What is the full range of answers of $m \pmod n$?
- *Example:* Try with $m \pmod 4$, replacing m by different numbers

Modulo

- What if I wanted to loop over the values 6, 7, 8, 9?
- What if I wanted to loop over the values 0, 2, 4, 6?
- What if I wanted to loop over the values 2, 4, 6, 8?

Modulo

- From this, a fundamental property of the modulo operator emerges: adding a multiple of the divisor to any dividend has no effect on the result of the modulus

□ *Example:*

$$4 \bmod 5 = 9 \bmod 5 = 24 \bmod 5 = -6 \bmod 5$$

Modulo

- Another property of modulo is the following:

$$a \times b \bmod n = (a \bmod n \times b \bmod n) \bmod n$$

- Example:

$$\begin{aligned} 14 \times 5 \bmod 3 &= (14 \bmod 3 \times 5 \bmod 3) \bmod 3 \\ &= (2 \times 2) \bmod 3 \\ &= 1 \end{aligned}$$

Modulo

- We can use modulo to calculate any value in a repeated cycle.
- *Example:* What is the last digit of 2^{401} ?