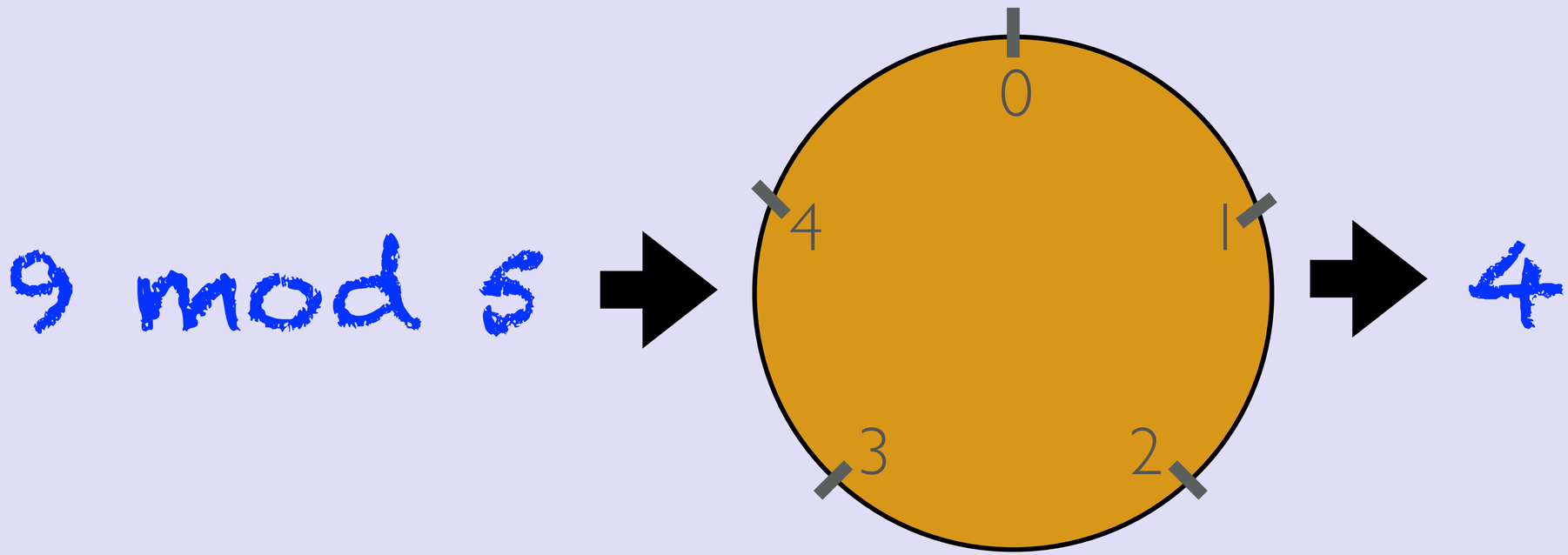
BLOCKCHAIN TUTORIAL 7

Modulo operation



BLOCKCHAIN TUTORIAL 7

Modulo operation

MODULO OPERATION

$$\frac{7}{5} = 1 \text{ remainder } 2$$

- If you are only are interested in the remainder, the mathematical notation is:
  $7 \bmod 5 \equiv 2$

- You pronounce it as: 7 modulo 5 is congruent to 2

- In this example the value 5 is called the modulus

- The purpose of applying a modulo operation is to keep the resulting value (remainder) within a certain range.

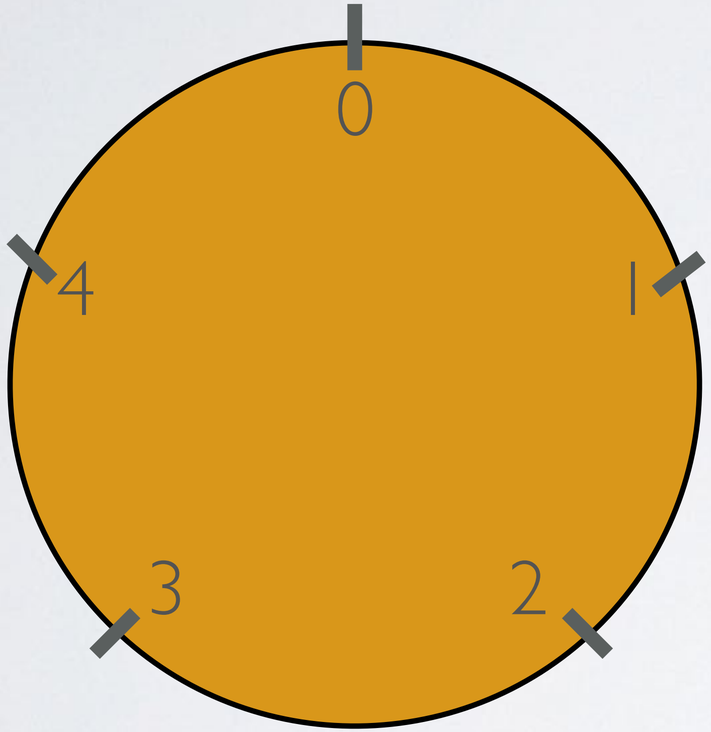
MODULO OPERATION

0 mod 5 ≡ 0	5 mod 5 ≡ 0	10 mod 5 ≡ 0	15 mod 5 ≡ 0
1 mod 5 ≡ 1	6 mod 5 ≡ 1	11 mod 5 ≡ 1	16 mod 5 ≡ 1
2 mod 5 ≡ 2	7 mod 5 ≡ 2	12 mod 5 ≡ 2	17 mod 5 ≡ 2
3 mod 5 ≡ 3	8 mod 5 ≡ 3	13 mod 5 ≡ 3	18 mod 5 ≡ 3
4 mod 5 ≡ 4	9 mod 5 ≡ 4	14 mod 5 ≡ 4	19 mod 5 ≡ 4

- n mod p = "remainder" = {0, …, p-1}
- Example: $\lambda^2 - x - x_G \pmod p$

MODULO OPERATION

- Modulo operation is also called a clock operation



$0 \bmod 5 \equiv 0$
$1 \bmod 5 \equiv 1$
$2 \bmod 5 \equiv 2$
$3 \bmod 5 \equiv 3$
$4 \bmod 5 \equiv 4$

$5 \bmod 5 \equiv 0$
$6 \bmod 5 \equiv 1$
$7 \bmod 5 \equiv 2$
$8 \bmod 5 \equiv 3$
$9 \bmod 5 \equiv 4$

MODULO OPERATION

- The purpose of this video is not to teach you how to do modulo arithmetic but just to explain what the purpose is of a modulo operation.

- Example:

  - $\lambda = (y_G - y) / (x_G - x) \pmod p$

  - $x_R = \lambda^2 - x - x_G \pmod p$

  - $y_R = \lambda(x - x_R) - y \pmod p$