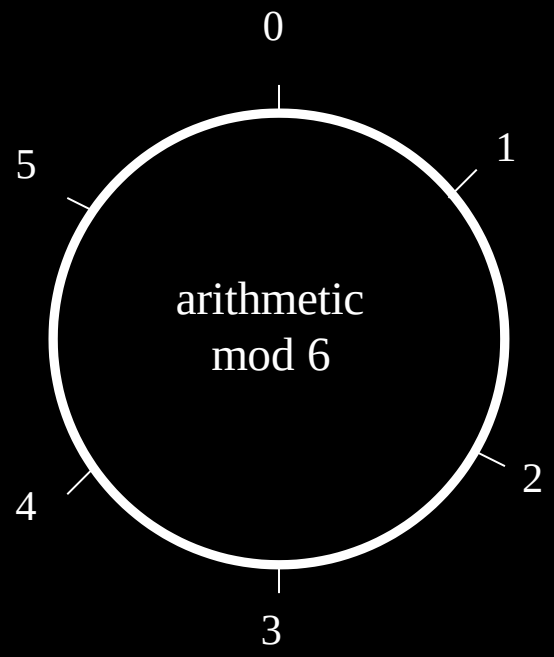
# Modular Arithmetic (Review)

# “Clock” Arithmetic

- For integers x andn, x mod n is the remainderof x n
- Examples
  - 7 mod 6 = 1
  - 33 mod 5 = 3
  - 33 mod 6 = 3
  - 51 mod 17 = 0
  - 17 mod 6 = 5



# A Note on Notation

- As computer scientists, we are used to seeing
  `7 mod 3 == 1`
- Mathematicians would more likely write
  `7 = 1 (mod 3)`
  and they might not bother with parenthesis
- You will see both forms in this class and your book. They mean the same thing

# Modular Addition

- Notation and facts
  - 7 mod 6 = 1
  - 7 = 13 = 1 mod 6
  - ((a mod n) + (b mod n)) mod n = (a + b) mod n
  - ((a mod n)(b mod n)) mod n = ab mod n
- Addition Examples
  - 3 + 5 = 2 mod 6
  - 2 + 4 = 0 mod 6
  - 3 + 3 = 0 mod 6
  - (7 + 12) mod 6 = 19 mod 6 = 1 mod 6
  - (7 + 12) mod 6 = (1 + 0) mod 6 = 1 mod 6

# Modular Multiplication

- Multiplication Examples
  - $3 \blacktriangledown 4 = 0 \pmod 6$
  - $2 \blacktriangledown 4 = 2 \pmod 6$
  - $5 \blacktriangledown 5 = 1 \pmod 6$
  - $(7 \blacktriangledown 4) \bmod 6 = 28 \bmod 6 = 4 \bmod 6$
  - $(7 \blacktriangledown 4) \bmod 6 = (1 \blacktriangledown 4) \bmod 6 = 4 \bmod 6$

# Additive Inverse

- Additive inverse of x mod n
  - the number that must be added to x to get 0 mod n
  - denoted -x
- -2 mod 6 = 4,
  since: 2 + 4 = 0
  mod 6

# Multiplicative Inverse

- Multiplicative inverse of x mod n
  - denoted $x^{-1}$
  - the number that must be multiplied by x to get 1 mod n
- $3^{-1}$ mod 7 = 5,
  since 3 ◆ 5 = 1 mod 7

# Modular Arithmetic Quiz

- Q: What is -3 mod 6?
- A: 3
- Q: What is -1 mod 6?
- A: 5
- Q: What is $5^{-1}$ mod 6?
- A: 5
- Q: What is $2^{-1}$ mod 6?
- A: No number works!
- Multiplicative inverse might not exist

# Relative Primality

- x and y are **relatively prime** if they have no common factor other than 1
- $x^{-1}$ mod y exists only when x and y are relatively prime
- $x^{-1}$ mod y is easy to find (when it exists) using the Euclidean Algorithm