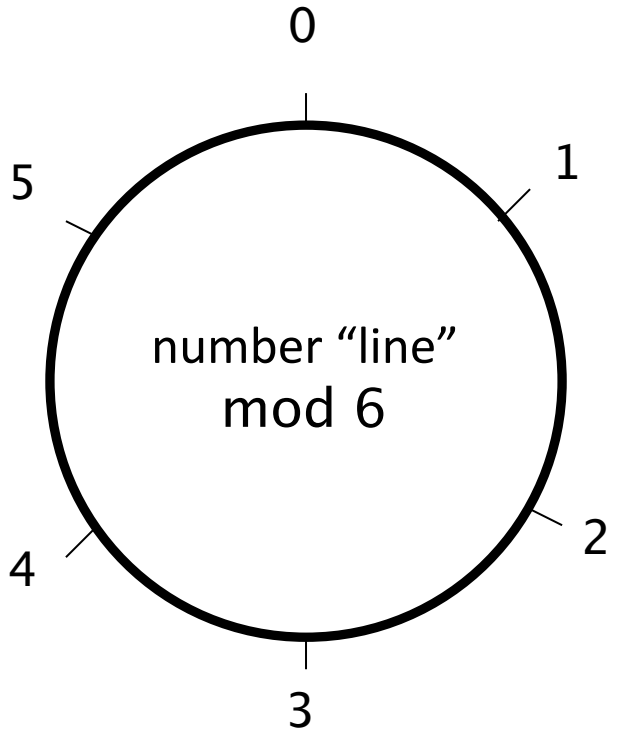
Modular Arithmetic

Clock Arithmetic

- For integers x and n, "x mod n" is the remainder when we compute x ÷ n
  - We can also say "x modulo n"

- Examples
  - 7 mod 6 = 1
  - 33 mod 5 = 3
  - 33 mod 6 = 3
  - 51 mod 17 = 0
  - 17 mod 6 = 5



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

Modular Inverses

- *Additive inverse* of $x \bmod n$, denoted $-x \bmod n$, is the number that must be added to x to get $0 \bmod n$
  - $-2 \bmod 6 = 4$, since $2 + 4 = 0 \bmod 6$
- *Multiplicative inverse* of $x \bmod n$, denoted $x^{-1} \bmod n$, is the number that must be multiplied by x to get $1 \bmod n$
  - $3^{-1} \bmod 7 = 5$, since $3 \cdot 5 = 1 \bmod 7$

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
- $x^{-1} \bmod y$ exists only when x and y are relatively prime
- If it exists, $x^{-1} \bmod y$ is easy to compute using Euclidean Algorithm
  - We won't do the computation here

Totient Function

- $\varphi(n)$ is "the number of numbers less than n that are relatively prime to n"
  - Here, "numbers" are positive integers
- Examples
  - $\varphi(4) = 2$ since 4 is relatively prime to 3 and 1
  - $\varphi(5) = 4$ since 5 is relatively prime to 1,2,3,4
  - $\varphi(12) = 4$
  - $\varphi(p) = p-1$ if p is prime
  - $\varphi(pq) = (p-1)(q-1)$ if p and q prime