CS 70 Discussion 3B

September 20, 2024

Modulo Operation

Basic Definition: $a \bmod m =$ remainder of a divided by m (ex. $14 \bmod 5 = 4$)
Residue Classes: $a \equiv b \pmod{m}$ means $(\exists k \in \mathbb{Z})(a = b + km)$ (i.e. $b - a$ is a multiple of m)

- In this case, we say that a and b are in the same "residue class" modulo m

Some useful formulas to note:

- $a + b \equiv (a \bmod m) + (b \bmod m) \pmod{m}$
- $a - b \equiv (a \bmod m) - (b \bmod m) \pmod{m}$
- $a \times b \equiv (a \bmod m) \times (b \bmod m) \pmod{m}$
- $a^b \equiv (a \bmod m)^b \pmod{m}$

Euclid's Algorithm

Problem: How do we easily get the greatest-common divisor (the largest integer that divides two numbers a and b) of two numbers?
Algorithm:

$$\gcd(a, b) = \begin{cases} \gcd(b, a \bmod b) & \text{if } b > 0 \\ a & \text{else} \end{cases}$$

Example:

$$\begin{aligned} \gcd(24, 42) &= \gcd(42, 24 \bmod 42) \\ &= \gcd(42, 24) \\ &= \gcd(24, 42 \bmod 24) \\ &= \gcd(24, 18) \\ &= \gcd(18, 24 \bmod 18) \\ &= \gcd(18, 6) \\ &= \gcd(6, 18 \bmod 6) \\ &= \gcd(6, 0) = 6 \end{aligned}$$

Inverses

An inverse of an integer a in modspace m is another integer a^{-1} such that:

$$a \times a^{-1} \equiv 1 \pmod{m}$$

Example: Inverse of 2 mod 5 is 3 (i.e. $2^{-1} \equiv 3 \pmod{5}$):

$$2(3) \equiv 6 \equiv 1 \pmod{5}$$

$a \pmod{m}$ has an inverse iff (if and only if) $\gcd(a, m) = 1$ (i.e. a and m are **coprime**). Multiplying by modular inverses is the way to emulate "division" in modspace.