Discussion 10

1. Recall the definition that for positive integer m and integers a, b $a \equiv b \pmod{m}$ means $m \mid a - b$ or (equivalently) a **mod** $m = b$ **mod** m.

(a) Prove that the congruence mod m relation is **reflexive** as a relation on $\mathbb{Z}$.

(b) Prove that the congruence mod m relation is **symmetric** as a relation on $\mathbb{Z}$.

(b) Prove that the congruence mod m relation is **transitive** as a relation on $\mathbb{Z}$.

2. We saw in class the computing powers (mod a prime) is a key step in many cryptographic protocols. Let's explore two algorithms to compute modular exponentiation.
Brute force approach: For $b, n, m \in \mathbb{Z}^+$, we can define b^n **mod** m recursively as

$$b^n \textbf{ mod } m = \begin{cases} b \textbf{ mod } m & \text{if } n = 1 \\ (b \cdot (b^{n-1} \textbf{ mod } m)) \textbf{ mod } m & \text{if } n > 1 \end{cases}$$

Using this definition, calculate 7^{17} **mod** 9.

Fast exponentiation: On page 254, Algorithm 5 we see the alternate algorithm

procedure *modular exponentiation*(b integer, $n = (a_{k-1}a_{k-2}\ldots a_1a_0)_2$, m positive integer)
$x := 1$
$power := b$ **mod** m
for $i := 0$ **to** $k - 1$
  if $a_i = 1$ **then** $x := (x \cdot power)$ **mod** m
  $power := (power \cdot power)$ **mod** m
return x

Using this definition, calculate 7^{17} **mod** 9.