1. Chapter 8 Congruences
   Properties:
   $a \equiv a$ (mod m)
   $a \equiv b$ (mod m) $\Rightarrow b \equiv a$ (mod m)
   $a \equiv b$ (mod m), $b \equiv c$ (mod m) $\Rightarrow a \equiv c$ (mod m)
   if $a \equiv b$ (mod m), $c \equiv d$ (mod m) $\Rightarrow$
   $a + c \equiv b + d$ (mod m)
   $a - c \equiv b - d$ (mod m)
   $ac \equiv bd$ (mod m)

2. Chapter 9,10

   (a) Fermat's Little Theorem
   If p is prime, and $p \nmid a$ then $a^{p-1} \equiv 1$ (mod p)

   (b) Euler's phi function:
   $\phi : \mathbf{N} \to \mathbf{N}, \phi = \#\{a|1 \leq a \leq m, gcd(a,m) = 1\}$
   For primes: $\phi(p) = p - 1$

   (c) Euler's Phi Formula:
   If gcd(a,m) = 1, $a^{\phi(m)} \equiv 1$(mod m)
   Prove:
   Suppose gcd(a,m) = 1. $b_n, 1 \leq n \leq \phi(m)$ represents all numbers that are co-prime to m.
   Consider A = $ab_1, ab_2, ab_3, \ldots, ab_{\phi(m)}$ (mod m) and B = $b_1, b_2, b_3, \ldots, b_{\phi(m)}$ (mod m). They have the same number of elements. If all elements in A are congruent to different number mod m, two set are the same.
   We prove by contradiction, suppose $ab_i \equiv ab_j$ (mod m)$\Rightarrow m|a(b_i - b_j) \Rightarrow m|(b_i - b_j) \Rightarrow b_i \equiv b_j$ contradicts!
   Then $b_1 b_2 \ldots b_{\phi(m)} \equiv ab_1 ab_2 \ldots ab_{\phi(m)}$(mod m)
   $\Rightarrow \prod_{i=1}^{\phi(m)} b_i \equiv a^{\phi(m)} \prod_{i=1}^{\phi(m)} b_i$ (mod m)
   since $b_i's$ are coprime to m, $\prod_{i=1}^{\phi(m)} b_i$ are coprime to m. $\Rightarrow 1 \equiv a^{\phi(m)}$ (mod m)