CS1231 Review 12

1. Modular Arithmetic

   - Definition: a is congruent to b modulo m, we write as $a \equiv b \mod m$, if $m \mid (a-b)$
   - Theorem. $a \equiv b \mod m$ iff $a \bmod m = b \bmod m$ iff $a = b + km \quad k \in \mathbb{Z}$
   - Theorem. $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$, $ac \equiv bd \mod m$, $a - c \equiv b - d \mod m$, $a^n \equiv b^n \mod m$, $n \in \mathbb{Z}^+$

2. 1 is NOT prime. 1 is NOT composite.