CS1231 Review 14

1. Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. An integer $\overline{a}$ such that $a \cdot \overline{a} \equiv 1 \mod m$ is called an **inverse of** a **modulo** m.

2. Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then the inverse of a modulo m exists iff $\gcd(a, m) = 1$.

   The inverse, if exists, is unique modulo m, i.e., if c, d are inverses, then $d \equiv c \mod m$.

3. (Fermat's Little Theorem) (FLT) If p is a prime and $a \in \mathbb{Z}$ such that $\gcd(p, a) = 1$, then $a^{p-1} \equiv 1 \mod p$.