Quiz 5 Solutions

written by Alvin Wan . alvinwan.com/cs70

Tuesday, February 9, 2016

This quiz does not count towards your grade. It exists to simply gauge your understanding. Treat this as though it were a portion of your midterm or final exam. "Intuition Practice" might be tricky; watch out for subtleties. "Proofs" will be challenging to start; develop an arsenal of *approaches* to starting a problem.

1 Intuition Practice

1. $6x = 2 \pmod 8$ has no solution. *Remember: In the mod universe, multiply by the multiplicative inverse and do not divide.*

   False. $x = 3$ is a solution. Note that although a multiplicative inverse does not exist, there is still a solution. Be careful.

2. Let c be a composite number with factors $F = \{x_0, x_1 ... x_n\}$. $\forall x_i \in \{0, 1 ... c-1\}, \exists y^{-1} \pmod c$ s.t. $y^{-1} \pmod c$ exists and is unique.

   False. $\forall x_i \in F$, there exists no multiplicative inverse. To easily see this, note that the $gcd(x_i \in F, c) = x_i$.

3. Let c be a composite number and p be a prime number where $p < c$ where $p \notin F$. $p^{-1} \pmod c$ exists and is unique.

   True. By construction, p is not a factor of c. In addition, p is itself prime, so it could not share a factor f, where $f < p$ with c. This means f is coprime with c, which implies a multiplicative inverse exists.