

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