Quiz 8 Solutions

written by Alvin Wan . alvinwan.com/cs70

Thursday, February 18, 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 Proofs

1. Prove or disprove that $x^y = x^{y(mod(p-1))}(modp)$. (Hint: Apply Fermat's Little Theorem)

   How do I start?

   Try to prove it first, and see if you land on a false step.

   Proof

   Let $y = a(p-1) + b$. We construct a and p so that $y = b(mod(p-1))$.

   $$\begin{aligned} & x^y(modp) \\ &= x^{a(p-1)+b}(modp) \\ &= x^{a(p-1)}x^b(modp) \\ &= (x^{p-1})^a x^b(modp) \end{aligned}$$

   By Fermat's Little Theorem, we know $x^{p-1} = 1(modp)$.

   $$\begin{aligned} &= 1^a x^b(modp) \\ &= x^b(modp) \\ &= x^{y(mod(p-1))} \end{aligned}$$

2. Prove or disprove that all polynomials in $GF(p)$, where p is prime, must have degree less than or equal to $p-2$. (Hint: Apply Fermat's Little Theorem)

   How do I start?

   Once again, attempt to prove it. The takeway from this problem is that you should keep in mind the boundary conditions for Fermat's Little Theorem.

"Proof"

By part (a), we know $x^y = x^{y(mod(p-1))}$ (mod p), where $y \geq p-1$ can be reduced to a number $\in 0, ...p-2$. However, there is boundary condition. Fermat's Little Theorem prohibits its base a from being 0. In other words, we cannot apply $a^{p-1} = 1$ (mod p), if $a = 0$. This theorem cannot be proved. We could formally justify this with a proof for the opposite or a counterexample.