Quiz 5 Solutions

written by Alvin Wan . alvinwan.com/cs70

Monday, September 12, 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.

1 Modular Arithmetic

1. (True or False) The solution to $2x = 3 \mod 7$ is less than 2.

   Solution: False. $x = \frac{3}{2}$ is not a valid numerical value in $\mod 7$. Instead, we should take the multiplicative inverse. $2^{-1} \mod 7 = 4$, so $x = 3(2^{-1}) = 12 = 5 \mod 7$.

2. Solve the following system of equations.

$$\begin{aligned} x - y &= 5 \mod 5 \\ -3x + 2y &= 6 \mod 5 \end{aligned}$$

   Solution: $x = y = 4$

   Solve the system of equations *almost* normally. First, take mod 5 for all numbers.

$$\begin{aligned} x + 4y &= 0 \mod 5 \\ 2x + 2y &= 1 \mod 5 \end{aligned}$$

   Plug in x and solve. Remember that to convert a negative n number into a number in $\mod p$, keep adding p to your negative number n until $0 \leq n < p$. (In the following example, $-6 = 4 \mod 5$).

$$\begin{aligned} 2(-4y) + 2y &= 1 \\ -6y &= 1 \\ 4y &= 1 \end{aligned}$$

   Note that at this point, it is *not* valid to say $y = \frac{1}{4}$, because $\frac{1}{4}$ doesn't exist in $\mod 5$!. We *do* have the multiplicative inverse of 4 though, where $4^{-1} = 4 \mod 5$. Thus, we have

$$\begin{aligned} 4y &= 1 \mod 5 \\ 4y(4^{-1}) &= 1(4^{-1}) \mod 5 \\ y &= 1(4) \mod 5 \\ y &= 4 \end{aligned}$$

Since $x - y = 0$, we know $x = y = 4 \mod 5$.

In the above example, you could have plugged in $x = y$ into the second equation to get the same answer. I used $x = -4y$ to briefly introduce converting negative numbers into numbers in the mod universe. As it turns out $x = -4y \mod 5$ is really $x = y \mod 5$ anyways.

3. Prove that $\forall n \in \mathbb{N}, (n-1) | -(n^2 + 3n + 2) \mod n$. (i.e., (n-1) *divides* $-(n^2 + 3n + 2)$).

   Solution: We know $-(n^2+3n+2) = -(n+1)(n+2) = (-n-1)(n+2)$. Since we're working in $\mod n$, adding n to a quantity does not change its value. Thus, we can state $(-n-1) + 2n = n - 1$. We then have that $-(n^2 + 3n + 2) = (n-1)(n+2)$. To formally state that $n - 1$ indeed divides $-(n^2 + 3n + 2)$. Since n is an integer, so is $n + 2$, so $\exists k \in Z, (n-1)k = -(n^2 + 3n + 2) \mod n$.