Crib 5

written by Alvin Wan . alvinwan.com/cs70

Monday, September 12, 2016

The crib sheet contains cheat-sheet worthy information but is not a substitute for lectures or for reading the notes. It also contains pointers and common mistakes.

1 Definition

- In a $\mod p$ universe, only the values $\{0, 1, ...p - 1\}$ exist. This means no negative numbers or fractions exist.

2 Multiplicative Inverse

- The multiplicative inverse of n in $\mod p$ (or, for short, $n^{-1} \mod p$) is defined so that $nn^{-1} = 1 \mod p$. (Say $p = 5$ and $n = 3$, then $3(3^{-1}) = 1 \mod 5$. We can see that $3^{-1} = 2 \mod 5$, as $3(2) = 6 = 1 \mod 5$. We will find an algorithm that computes the multiplicative inverse in the next lecture.)
- The multiplicative inverse of n in $\mod p$ exists if and only if n is co-prime with p. i.e., n and p do not share any common factors greater than 1.
- Even if n and p are not co-prime, the equation may still have a solution. For example, $2x = 4 \mod 6$ has a solution, even though 2 is not co-prime with 6. (Of course, it is easy to see that $x = 2$ works.)