Crib 6

written by Alvin Wan . alvinwan.com/cs70

Monday, September 26, 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 Fermat's Little Theorem

- If p is prime, we have that $a^p \equiv a(\text{mod p})$.
- If p is prime, p does not divide a, and $a > 0$, then $a^{p-1} \equiv 1(\text{mod p})$.
- By Fermat's Little Theorem, we then have that $a^x \equiv a^{x(\text{mod (p-1)})}(\text{mod p})$

2 Chinese Remainder Theorem

1. For many i, where $x = a_i \mod n_i$ and all n_i are pairwise co-prime, CRT allows us to compute a unique $x \mod \Pi_i n_i$ that satisfies all equations.