Ground Rules. You may choose to work with one other student if you wish. Only one submission is required per group, please ensure that both group members names are on the submitted copy. Work must be submitted in hard copy by the start of class on November 6, 2018. Questions marked as COSC 583 are required for those enrolled in the 583 section. If you are in the 483 section you are more than welcome to attempt any of them, extra credit will be awarded for correct answers.

1. mod mod
Let $p, N$ be integers with $p|N$. Prove that for any integer $X$, $[[X\mod N]\mod p]=[X\mod p]$. Show that, in contrast, $[[X\mod p]\mod N]$ need not equal $[X\mod N]$.

2. Compact Exponentiation
Compute the following by hand (show your work, machine assistance not allowed, you should not use a fast exponentiation algorithm, there is a mathematical trick to each):

- $104^{453}\mod 103$
- $33^{40}\mod 41$
- $2^{38}\mod 15$

3. Euler phi function
- Let $p$ be prime and $e \geq 1$ ($e$ is an integer). Show that $\phi(p^e) = p^{e-1}(p - 1)$.
- Let $p$ and $q$ be relatively prime. Show that $\phi(pq) = \phi(p)\phi(q)$. Hint: use the Chinese remainder theorem.

4. Alternative DH Complete problem 11.6 from the textbook.

*583 only* 5. Flipping Coins Complete problem 11.8 from the textbook.