MATH 470 Homework 9 (Due November 15 **on Gradescope**)

Instructions:

- FOR 5 POINT QUESTIONS, IF YOU LEAVE AN ANSWER BLANK, YOU WILL AUTOMATICALLY RECEIVE 2/5 POINTS. ANY ATTEMPTED SOLUTION WILL BE GRADED AS USUAL (AND POSSIBLY GET LESS THAN 2/5 POINTS). DOES NOT APPLY TO BONUS QUESTIONS.
- The writing of your homework submission should be done entirely on your own and you should be able to justify all of your writing in your own words.
- Show your work and write legibly. If there is any difficulty in reading or understanding your submission, or if any nontrivial steps are missing in your work, then points may be deducted.
- When you upload your submission to Gradescope, **make sure you match the correct page(s) for each question**. Otherwise your submission may not be graded, or points may be deducted.
- You may use an online calculator or code for the following operations:
  - add, subtract, multiply, quotient, remainder, rounding, non-modular square roots
  - (Extended) Euclidean Algorithm, fast powering

Required problems (in the SECOND edition of textbook: "An Introduction to Mathematical Cryptography", Second Edition, by Hoffstein, Pipher, and Silverman.)

1. (5 points) 5.39
2. (5 points) 5.44(b)

For Q3-6, consider the following protocol:

> Let p be a large prime of the form $p = 2q + 1$ where q is a prime. Let $g \in (\mathbb{Z}/p\mathbb{Z})^*$ be an element of order q. Let $\langle g \rangle$ denote the set $\{1, g, g^2, g^3, \dots, g^{q-1} \mod p\}$. (note that g is not a primitive root mod p, and $\langle g \rangle$ only contains half of the numbers in $(\mathbb{Z}/p\mathbb{Z})^*$). Assume that the discrete logarithm problem for p, g is hard. In other words, assume that there is no efficient algorithm that can compute, for any given $A \in \langle g \rangle$, an integer a such that $g^a \equiv A \mod p$.
> Let $A \in \langle g \rangle$. Peggy wants to convince Victor that she knows an integer a such that $g^a \equiv A \mod p$.
>
> - Peggy chooses a random integer $c \in \mathbb{Z}/q\mathbb{Z}$, computes $C = g^c \mod p$, and sends the **commitment** C.
> - Victor chooses a random integer $h \in \mathbb{Z}/q\mathbb{Z}$, and sends the **challenge** h.
> - Peggy computes $r = c + ah \mod q$, and sends the **response** r.
> - Victor **accepts** if $g^r \equiv C \cdot A^h \mod p$, and **rejects** otherwise.

3. (5 points) Let x be an integer with $x \not\equiv 0 \mod q$. Prove that there exists an integer y such that $g^{xy} \equiv g \mod p$.
4. (5 points) Prove that the above protocol satisfies **completeness**; that is, prove that if Peggy does know a and if both parties follow the protocol, then Victor always accepts.
5. (5 points) A *transcript* is a tuple (C, h, r) where $C \in \langle g \rangle$, $h \in \mathbb{Z}/q\mathbb{Z}$, and $r \in \mathbb{Z}/q\mathbb{Z}$. A transcript (C, h, r) is *valid* if $g^r \equiv C \cdot A^h \mod p$.
   Prove that if you are given two valid transcripts (C, h_1, r_1) and (C, h_2, r_2) with $h_1 \not\equiv h_2 \mod q$, then you can efficiently compute a. (This property is called **special soundness**)
6. (5 points) Prove that the above protocol satisfies **honest verifier zero knowledge**; that is, prove that there is an efficient algorithm which, without knowledge of a, can produce transcripts that are indistinguishable from transcripts of honest interactions between Peggy (who knows a) and Victor.