MATH 470 Homework 10 (Due November 29 **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
- You may NOT use online tools/libraries for elliptic curve operations. These should all be implemented from scratch, if you decide to use a computer.

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

1. 6.2(a,b) (don't do the bonus)
2. 6.6(b)
3. 6.9
4. 6.11(c)
5. 6.14(a,b)
6. 6.21(b)

Suggested practice problems (do not submit): 6.5(b,d), 6.7, 6.8, 6.16, other parts of the required problems above. You should also think about the elliptic curve versions of the zero-knowledge proofs we saw based on discrete logs.