MATH 470 Homework 8 (Due October 25 **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. (10 points) 3.36 (all parts)
2. (5 points) Use the Tonelli-Shanks algorithm to compute a square root of 6 modulo 97 (note 97 is prime).
3. (5 points) Using the fact that $2021 = 43 \cdot 47$ and that 43 and 47 are both primes, use the Tonelli-Shanks algorithm and the Chinese remainder theorem to compute a square root of 6 mod 2021.
4. (5 points) Prove or disprove the following statement:

   Let $N = pq$ where p, q are distinct odd primes. If a, b are integers such that $a^2 \equiv b^2 \pmod{N}$ and $a \not\equiv \pm b \pmod{N}$, then $\gcd(a - b, N)$ or $\gcd(a + b, N)$ gives a nontrivial factor of N.
5. (5 points) Read Example 3.69 in the textbook. Explain (in more detail than in Example 3.69) why $(-1)^{\mathrm{dlog}_g(h)} = \left(\frac{h}{p}\right)$.
6. (Bonus 5 points) 3.40