MATH 470 Homework 6 (Due October 12 **on Gradescope**)

Instructions:

- 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) Let $N = pq$ be the product of two distinct primes. Let e, d be integers such that $ed \equiv 1 \mod \phi(N)$. Prove that for every integer m, we have $m^{ed} \equiv m \mod N$.
   (note: If $\gcd(m, N) = 1$, then this follows from the Proposition from class that $m^{\phi(N)} \equiv 1 \mod N$. The purpose of this problem is to handle the other cases, thus proving that RSA decryption always returns the original message.)
2. (5 points) 3.26(d)
3. (5 points) 3.29 (round to 4 significant digits)
4. (5 points) Implement Pollard's $p - 1$ algorithm on a computer to factor N:

   $$N = 340510176929609558738506407941198102081020749940944635553628097992090306553579338501$$

   (I suggest Python, but you can use any standard language)
5. (5 points) 1.36(d)
6. (5 points) Let k be a positive integer. What is the number of square roots of 1 modulo 2^k? In other words, determine the number of integers x with $0 \leq x \leq 2^k - 1$ that satisfy $x^2 \equiv 1 \mod 2^k$. (the answer may depend on k)
7. (Bonus 5 points) Let p be an odd prime and let b be an integer not divisible by p. Prove that for every positive integer e, the congruence $X^2 \equiv b \mod p^e$ has either 0 or 2 solutions in $\mathbb{Z}/p^e\mathbb{Z}$.
   (hint: use 1.36(a) (HW3 Q4) and HW4 Q5. See also 1.37)