MATH 470 Homework 3 (Due September 13 **on Gradescope**)

Instructions:

- 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.
- For questions marked $*$ (e.g. 6^*.), you may write your own code (in any standard language) to solve the problem. But in this case you must write the code **from scratch** and attach a copy or screenshot of the working code together with the output in your submission.
  The only "built-in" mathematical functions you can use in the code are:
  - basic arithmetic operations: add, subtract, multiply, quotient, remainder

  Any other mathematical function you want to use must be built by you using the above.
  If your submission uses other built-in library functions (e.g. gcd in numpy), you will get 0. If it is noticed that the output of your submitted code does not match your answer, this will be considered a violation of the Aggie Honor Code.

Required problems: (submit on Gradescope)

1. (5 points) 1.32(b) (do this by hand)
2. (5 points) 1.33(a)
3. (5 points) 1.35
4. (5 points) 1.36(a)
5. (10 points)
   (a) Let $p = 13$ and let $g = 2$. Note that p is prime and that g is a primitive root modulo p.
   Make a list of the powers of g and their orders modulo p (i.e., for each $a \in \{1, 2, 3, \ldots, 12\}$, write down $g^a \mod p$ and the order of g^a modulo p). What are all the primitive roots modulo p? Compute $\phi(p-1)$, where ϕ is the Euler's totient function.

   (b) Let p be a prime, let g be a primitive root modulo p, and let a be an integer. Prove that the order of g^a modulo p is exactly $\dfrac{p-1}{\gcd(a, p-1)}$. Explain why this implies that the number of primitive roots modulo p is exactly $\phi(p-1)$, assuming that a primitive root g modulo p exists.
   (Looking over your work in part (a) may help you gain some intuition).
6. (Bonus 5 points) You may assume that the following integers p and q are primes:

   $$p = 12345678901234567890123456789012345678901234567890123456789012345678901234567890123459287$$
   $$q = 61728394506172839450617283945061728394506172839450617283945061728394506172839450617729643$$

   Also note that $p = 2q+1$. Find the smallest positive integer g that is a primitive root modulo p. (hint: use exercise 1.35).
   If you are writing code, and if you are computing large powers, you will have to implement a powering algorithm yourself. (if you use a built-in power function, you will get 0)

Suggested practice problems (do not submit): 1.29, 1.34, 1.36(b-d), 1.38