Homework 7

Due: Friday, April 5 at noon

Instructions: Submit a pdf of your solutions to the HW 7 assignment on Gradescope. **You must complete the process by associating the proper page(s) to each question.** (If you fail to do so, you may earn "not assessable" on any problems that do not have solutions matched to them.)

On this assignment, the main learning objectives being assessed and the grading criteria for each problem is included under the problem statement. If you are unsure about the meaning of a criterion, ask Dr. Burson.

1. Determine whether or not 3 is a primitive root modulo 19 without computing all of the powers of 3 modulo 19.
   Learning objectives: (1) Use the theorem connecting orders and primitive roots modulo m to determine if an integer is a primitive root modulo another integer. (2) Use the theorem about possible orders modulo m to compute the order of an element with as few computations as possible.
   Grading Criteria: Final answer is correct and the work leading up to it is clear, legible, and written for the audience of other MATH 5248 students; Any theorems used are clearly identified (it should be clear where you used the theorems mentioned in the learning objectives); No major computational, logical, factual, or semantic errors in the work.

2. Explain why 6 is not a primitive root modulo 34 without computing *any* of the powers of 6 modulo 34.
   Learning objectives: (1) Demonstrate understanding of the requirements for being a primitive root modulo m.
   Grading Criteria: Final answer is correct and the work leading up to it is clear, legible, and written for the audience of other MATH 5248 students; A connection to the concept of units is made in the explanation; No major computational, logical, factual, or semantic errors in the work.

3. Prove that, if a is a primitive root modulo p, then a^{-1} (the multiplicative inverse of a modulo p) is also a primitive root modulo p.
   Learning objectives: (1) Use the theorem connecting primitive roots to orders in a proof. (2) Write a clear and correct proof by contradiction.
   Grading criteria: Proof is clear, legible, and written following mathematical conventions (as explained in the writing guidelines); Proof clearly and correctly cites any theorems and definitions used (it should be clear if a claim is due to a theorem or a definition); Proof does not use any theorems that have not been covered in MATH 5248; Proof correctly uses either properties of modular congruences or the division algorithm, including proper notation.

4. Bob and Alice would like to use the Diffie-Hellman Key Exchange to agree on a session key k. Alice and Bob agree on the prime 6829 and that the base 2 modulo 6829. Bob chooses a secret random number x and tells Alice that $2^x \% 6829$ is 5792. Alice chooses 3 as her secret exponent. Answer the following questions without computing the value of x.

   (a) What is the shared secret key k that Alice and Bob will be using?

   (b) You are able to gain access to the network Alice and Bob are using to communicate, so you decide to implement a interceptor attack with exponent $c = 10$. What key does Bob think he and Alice agreed to? What key does Alice think they agreed to?

   Learning objectives: (1) Implement the method of Diffie-Hellman Key Exchange. (2) Implement an interceptor attack on Diffie-Hellman Key Exchange.
   Grading criteria: Final answer is correct and the work leading up to it is clear, legible, and written for the audience of other MATH 5248 students; Work for part (a) does not require one to know the value of x; No major computational, logical, factual, or semantic errors in the work.