Suggested reading: Trappe-Washington 3.7, 7.1, 7.2 (stopping before 7.2.1), 7.4, 7.5, 3.9

1. (a) Let p be a positive prime. Define a *primitive root modulo p.*
   (b) Identify all primitive roots modulo 11. Is your solution consistent with the claim that there are $\phi(\phi(p))$ primitive roots modulo p?
   (c) We stated the *Primitive Root Theorem*: If p is prime, then there is at least one primitive root modulo p. Show that this result does not hold for composite n: if n is composite, then there may not be unit that is a multiplicative generator (ie, primitive root) of the set of units modulo n. *Hint:* Check the units modulo 8.

2. In this question, you will prove the following result which appeared in class and is given in Chapter 3.7 of the textbook. You are welcome to read the proof on page 84, but your solution must be written in your own words.

   Theorem 1.1. *Let p be a positive prime and g be a primitive root modulo p.*

   1. Let n be an integer. Then

   $$g^n \equiv 1 \pmod{p} \qquad \text{if and only if} \qquad n \equiv 0 \pmod{p-1}.$$

   2. If j and k are integers, then

   $$g^j \equiv g^k \pmod{p} \qquad \text{if and only if} \qquad j \equiv k \pmod{p-1}.$$

3. Trappe–Washington Chapter 3 Question 20.

4. Trappe–Washington Chapter 3 Question 21. This question develops a method for finding primitive roots.

5. (a) Define the *discrete logarithm problem* and the function $L_\alpha(\beta)$.
   (b) Explain why we can easily determine the parity of $L_\alpha(\beta)$ when α is a primitive root.
   (c) Trappe–Washington Chapter 7 Question 3.

6. (a) Describe the Diffie–Hellman Key Exchange (Chapter 7.4).
   (b) Trappe–Washington Chapter 7 Question 10.

7. (a) Describe the ElGamal public key cryptosystem (Chapter 7.5).
   (b) Trappe–Washington Chapter 7 Question 11.

8. At the end of Chapter 3.9 is stated the following principle:

   > Suppose $n = pq$ is the product of two primes congruent to 3 (mod 4), and suppose that y is a number relatively prime to n which has a square root modulo n. Then finding the four solutions $x = \pm a, \pm b$ to $x^2 \equiv y \pmod{n}$ is computationally equivalent to factoring n.

   (a) Explain why if $n = pq$ is the product of *any* two primes p, q, then knowing four square roots of a unit $y \pmod{n}$ enables us factor n.
   (b) Conversely, explain how (if p and q are both congruent to $3 \pmod{4}$) we can determine all square roots of y modulo $n = pq$. Include the statement of the main proposition in Chapter 3.9.
   (c) Alice and Bob are communicating secretly using the RSA cryptosystem with modulus $n = pq = 830429$. Suppose you learn that 500, 100 424, 730 005, and 829 929 are all square roots of 250 000 modulo n. Find p and q. Show your work.

9. Trappe–Washington Chapter 3 Question 25.

10. (**Not for credit**) What topic have you chosen for your WIM? Your answer is non-binding, but please do start thinking about your WIM topic and the specifics of what you might want to include in the paper.

11. (**Bonus**). Trappe–Washington Chapter 3 Question 27.