Name: _____

Read and take notes on 7.3 Primitive Roots, Discrete Logs.

Reading Questions

1. Complete the sentences to finish the definitions.

   (a) Given a positive integer n, for an integer g to be a **primitive root modulo** n means that (*for all ... there exists ... such that ...*)

   (b) Given a positive integer n, an integer g, an integer x with $\gcd(x, n) = 1$, a **discrete logarithm of** x **base** g **modulo** n is an integer ℓ with the following property:

   (c) For g, a primitive root modulo n, the **exponent** or **order** of g is ...

2. (a) Explain, in your own words, why 3 is a primitive root modulo 7. (This is the example given in the text.)

(b) For $x = 1, 2, 3, 4, 5, 6$, find the discrete log of x with base 3 modulo 7.

(c) What is the order of 3, as a primitive root modulo 7?

3. As discussed in the text, there are no primitive roots modulo 8. Why is it sufficient to check that none of 1, 3, 5, 7 are primitive roots modulo 8? In other words, why are 1, 3, 5, and 7 the only possibilities for primitive roots modulo 8?

4. Circle the integers n in the list below for which there exists at least one primitive root modulo n.

2 4 6 9 12 16 2 18 22 50 81 98

5. What struck you in this reading? What is still unclear? What remaining questions do you have?