Math 316, 13.5, 13.6 Strong Pseudoprimes and the Miller-Rabin Test

Name: _____

Read and take notes on 13.5 and 13.6 Strong Pseudoprimes and the Miller-Rabin Test.

Reading Questions

1. State the definition of a strong pseudoprime base b. (Note that this definition actually begins with the sentence prior to the sentence containing the boldface words "strong pseudoprime.")

2. Show that the smallest Carmichael number (561) is *not* a strong pseudoprime base 2.

3. What is the *idea* behind the Miller-Rabin Test?

4. Find all x in $\mathbb{Z}/8$ satisfying $x^2 = 1$.

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