

Name: _____

Read and take notes on Sections 19.2, Random Squares Factoring.

Reading Questions

1. Briefly explain, in your own words, how to find a factor of n if you have x, y such that $x^2 = y^2 \pmod n$ but $x \not\equiv \pm y \pmod n$.

2. How many square roots does $b = 4$ have modulo n , for
 - (a) $n = 9$

 - (b) $n = 15$

 - (c) $n = 101$

 - (d) $n = 105$

3. Find all square roots of 4 modulo 45 using Sun Ze's Theorem.

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