Name: _____

Read and take notes on 13.3 and 13.4 Euler Pseudoprimes and the Solovay-Strassen Test.

Reading Questions

1. (a) State the definition of the quadratic (Legendre) symbol for an odd prime p.

   (b) State the definition of the extended quadratic (Jacobi) symbol for an integer n with prime factorization $2^{e_0}p_1^{e_1}\dots p_k^{e_k}$, where p_i, $1 \le i \le k$ are distinct odd primes.

2. (a) What is an Euler pseudoprime base b?

   (b) What does it mean that there are no Euler-pseudoprime analogues of Carmichael numbers?

3. (a) Explain how the Solovay-Strassen Test can correctly indicate, with certainty, that a number is composite.

(b) Describe the process by which the Solovay-Strassen Test indicates that a number is prime.

(c) When the Solovay-Strassen Test indicates that a number is prime, how confident should we be that the number really is prime?

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