Name: _____

Read and take notes on the introduction to Chapter 13, Section 13.1 Fermat Pseudoprimes, and Section 13.2 Non-Prime Pseudoprimes.

Reading Questions

1. Make sure you are familiar with the following terminology: pseudoprime, witness, false witness/liar, Fermat pseudoprime, Fermat pseudoprime base b, Fermat witness, Fermat false witness/liar, Carmichael number.

2. What can we gain by 'sacrificing' certainty in primality testing? Why does this matter for modern cryptosystems?

3. What does Fermat's Little Theorem say? Give two equivalent ways of stating the result. (Make sure to include the quantifiers at the beginning of the sentences!)

4. True or false, with explanations.

   (a) If an odd integer n is prime, then $2^{n-1} = 1 \bmod n$.

   (b) An odd integer n is prime if $2^{n-1} = 1 \bmod n$.

(c) If $b^{n-1} = 1 \bmod n$ for all b relatively prime to n, then n is prime.

5. (a) Give an example of a non-prime Fermat pseudoprime. (There are eight listed in Section 13.1.)

(b) Use the first proposition in Section 13.2 to generate another non-prime Fermat pseudoprime from the one you gave in (a). (Give a formula for this number rather than trying to write out all the digits.)

(c) Use the second proposition in Section 13.2 to generate another non-prime Fermat pseudoprime.

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

Math 221, Crypto: 10.8 Euler's Criterion, 12.2A The Legendre Symbol

Name: _____

Read and take notes on Section 10.8, Euler's Criterion, focusing on the Corollary (Euler's Criterion), and the beginning of Section 12.2, Quadratic Symbols, just the part about the Legendre symbol, on page 163.

Reading Questions

1. Make sure you know the statement of Euler's Criterion (as described in the Corollary in Section 10.8) and the definition of the quadratic (Legendre) symbol.

2. (a) List the elements in $(\mathbb{Z}/7)^\times$, the set of units for $\mathbb{Z}/7$.

   (b) For each $x \in (\mathbb{Z}/7)^\times$, compute x^2. (Compute modulo 7.)

   (c) Which elements of $(\mathbb{Z}/7)^\times$ are squares in $(\mathbb{Z}/7)^\times$? (I.e. which elements occur as outputs of the squaring function?)

   (d) For each $y \in (\mathbb{Z}/7)^\times$, compute y^3. (Again, compute modulo 7.)

   (e) For which $y \in (\mathbb{Z}/7)^\times$ do we have $y^3 = 1$?

   (f) Do your results agree with the conclusion of Euler's Criterion? (Note that $3 = (7-1)/2$.)

3. Use Euler's Criterion to determine the following. (You can use *Mathematica* to do the exponentiation modulo 101.)

   (a) whether 2 is a square modulo 101

   (b) whether 14 is a square modulo 101

4. Use the previous problem to evaluate the Legendre symbols:

   (a) $\left(\frac{2}{101}\right)_2 =$

   (b) $\left(\frac{14}{101}\right)_2 =$

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

Name: _____

Read and take notes on the second part of Section 12.2, on the Jacobi symbol and Section 12.3, Multiplicative Property.

Reading Questions

1. Make sure you know the definition of the extended quadratic (Jacobi) symbol and the multiplicative property of quadratic symbols.

2. Consider $n = 1155$.

   (a) By hand, factor n as the product of several small primes.

   (b) Use the prime factorization of n and the definition of the Jacobi symbol to write $\left(\frac{b}{n}\right)_2$ as a product of Legendre symbols $\left(\frac{b}{p_1}\right)_2$, $\left(\frac{b}{p_2}\right)_2$, ..., where p_1, p_2, ... are prime.

3. Consider $n = 5625$.

   (a) By hand, factor n as the product of several small primes.

   (b) Use the prime factorization of n and the definition of the Jacobi symbol to write $\left(\frac{b}{n}\right)_2$ as a product of Legendre symbols $\left(\frac{b}{p_1}\right)_2$, $\left(\frac{b}{p_2}\right)_2$, ..., where p_1, p_2, ... are prime.

   (c) Find $\left(\frac{2}{5625}\right)_2$ without any additional computation.

4. (a) Use Euler's criterion to calculate $\left(\frac{2}{7}\right)_2$ $\left(\frac{3}{7}\right)_2$, $\left(\frac{2}{11}\right)_2$, and $\left(\frac{3}{11}\right)_2$.

   (b) Use the definition of the Jacobi symbol to calculate $\left(\frac{2}{77}\right)_2$ and $\left(\frac{3}{77}\right)_2$.

   (c) Use the multiplicative property of quadratic symbols to calculate $\left(\frac{6}{7}\right)_2$, $\left(\frac{6}{11}\right)_2$, and $\left(\frac{6}{77}\right)_2$.

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

Name: _____

Read and take notes on Sections 12.4 and 12.5, Quadratic Reciprocity and Fast Computation.

Reading Questions

1. Make sure you know the statements of both laws of quadratic reciprocity (Gauss' quadratic reciprocity and quadratic reciprocity for Jacobi symbols) as well as the corollary to quadratic reciprocity for Jacobi symbols.

2. Use Gauss' quadratic reciprocity to determine:

   (a) whether -1 is a square modulo the primes $p = 3, 5, 7, 11$.

   (b) whether 2 is a square modulo the primes $p = 3, 5, 7, 11$.

   (c) whether 7 is a square modulo the prime 541.

3. For each pair (m, n), use the law of quadratic reciprocity for Jacobi symbols to determine whether or not $\left(\frac{m}{n}\right)_2 = \left(\frac{n}{m}\right)_2$. (Note that you can do this without computing any Jacobi symbols.)

   (a) $m = 5$, $n = 9$

(b) $m = 11$, $n = 15$

(c) $m = 81$, $n = 101$

4. (a) About how many steps does it take to evaluate $\left(\frac{m}{n}\right)_2$, for m, n odd numbers with $1 < m < n$, using quadratic reciprocity?

   (b) What "hard" computation would be necessary to evaluate the Jacobi symbol $\left(\frac{m}{n}\right)_2$, without using quadratic reciprocity?

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

Math 221, Crypto: 13.3, 13.4 Euler Pseudoprimes and the Solovay-Strassen Test

Name: _____

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

Reading Questions

1. State the definition an Euler pseudoprime base b.

2. What two fast algorithms ensure that we can quickly compute both sides of the congruence in the criterion in this definition, thus making the criterion worthwhile?

3. True or false, with reasons.

   (a) If n is an Euler pseudoprime base b, then n is a Fermat pseudoprime base b.

   (b) If n is a Fermat pseudoprime base b, then n is an Euler pseudoprime base b.

4. If n is composite, what percentage of the bases b in the range $0 < b < n$ do we expect to be Euler witnesses to the compositeness of n?

5. (a) Suppose we run the Solovay-Strassen test for a number n with 5 bases $b_1, b_2, \ldots b_5$, where $1 < b_i < n-1$, and for all of these bases, n is an Euler pseudoprime. What is the (heuristic) probability that n is actually prime?

   (b) Suppose we continue to run the Solovay-Strassen test for the same n, with additional bases $b_6, b_7, \ldots, b_{10}$, where $1 < b_i < n-1$, and for four of these bases n is an Euler pseudoprime. (So, in total, n is an Euler pseudo-prime for 9 of the 10 bases we checked.) What can you conclude? Is your conclusion certain?

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

Math 221, Crypto: 9.6, 10.3 Square Roots mod p and mod n

Name: _____

Read and take notes on Section 9.6, Square Roots mod p and Section 10.3, Composite Moduli.

Reading Questions

1. Reread the theorem in Section 9.6 and the first remark following it.
   (a) What condition must the prime p satisfy, in order for the theorem to apply?

   (b) What condition must the number y satisfy, in order for the theorem to apply?

   (c) What is the number x called?

2. Reread the second remark in Section 9.6. Fill in the blank:

   The principal square root is the square root which is itself a _____ .

3. Find the principal square root of 2 modulo 7, as outlined below.
   (a) Check that 7 is the right kind of prime.

   (b) Check that 2 is a square modulo 7. (Compute the Legendre symbol using quadratic reciprocity.)

   (c) Use the formula in the theorem to find the principal square root of 2 modulo 7.

   (d) Check that your answer in (c) is a square root of 2 by squaring it and reducing modulo 7.

   (e) Check that your answer (c) is itself a square modulo 7 by computing the Legendre symbol.

4. Find 4 distinct square roots of 1 modulo 15, as outlined below.

   There are two obvious square roots of 1 modulo 15: $x = \pm 1 \bmod 15$. To find the other two we need to do a little work.

   (a) Solve the system of congruences: $x = 1 \bmod 3$ and $x = -1 \bmod 5$. (Use the method of 10.2.)

   (b) Check that your solution from (a) is a square root of 1 modulo 15.

   (c) To find the last square root of 1, simply take your solution from (a) and multiply by (-1).

   (d) List four integers x in the range $0 \leq x \leq 14$ such that $x^2 = 1 \bmod 15$.

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

Name: _____

Read and take notes on the first part of Section 14.3 Oblivious Transfer, up to and including the Remark on page 185.

Reading Questions

1. Reread the first two paragraphs in the section on oblivious transfer.

   (a) Describe, in your own words, the *simple version* of oblivious transfer.

   (b) Describe, in your own words, the *more complicated version* of oblivious transfer.

2. Reread the description of a mathematical implementation of the simple version of oblivious transfer. In this case, what is the secret? Why can't Bob simply guess the secret?

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