Math 316, Intro., 1.1 Shift Cipher, 1.2 Reduction/Division Algorithm, 1.3 One Time Pad

Name: ____

Read the introduction and Sections 1.1-1.3, The Shift Cipher, Reduction/Division Algorithm, and The One Time Pad. Read carefully, marking up your copy of the text and taking notes.

Reading Questions

1. Make sure you are familiar with the following terms from the introduction: cryptosystem, cipher, encryption, decryption, plaintext, ciphertext, key, code, encode, symmetric cipher, asymmetric cipher.

2. What are the four types of attacks on a cryptosystem? Describe them in your own words.

3. Make sure you are familiar with the following terms from Section 1.1: shift cipher, Caesar cipher, monoalphabetic cipher.

4. Why is a shift cipher very easy to break? In what context is a shift cipher completely effective?

5. The words in bold face in Section 1.2 are terms that you should know. In particular, make sure you know the meaning of reduction modulo a nonzero integer m, the quotient and remainder in the division algorithm, and a multiplicative inverse modulo m.

6. Compute the reduction of 16 modulo 5: $16 \,\%\, 5$.

7. How is the key for OTP different from the key for a shift cipher? Look again at the example encrypting the word ‘impossible’ using OTP. What is the key in this example?

8. Explain what it means for the OTP to be *polyalphabetic*. Use the example in the text (encrypting ‘impossible’) to illustrate the polyalphabetic nature of the OTP.

9. In your own words, explain the advantages and disadvantages of the OTP in comparison to the shift cipher.

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

Math 316, 1.4, 1.5, 1.6 Divisibility, Multiplicative Inverses, and Integers mod m

Name: ____

Read and take notes on Section 1.4, Divisibility, Section 1.5, Multiplicative Inverses, and Section 1.6 The Integers mod m.

Reading Questions

1. Make sure you are familiar with the terminology and notation introduced in Section 1.4, especially the following terms: divides/divisor, properly divides/proper divisor, relatively prime, coprime, greatest common divisor.
2. The theorem on the greatest common divisors of two integers is important. Make sure you have it in your notes, word for word.
3. What is the greatest common divisor of 4 and 6? By trial and error, write this number in the form given in the theorem, i.e. find two integers, x and y, such that $\gcd(4, 6) = 4x + 6y$.
4. Carefully reread the first proposition in Section 1.5. (Make sure it's in your notes, word for word.)
   (a) Which of the integers 0, 1, 2, 3, . . . , 23 have a multiplicative inverse modulo 24? (You don't need to find the inverses to do this.)

   (b) Which of the integers 0, 1, 2, 3, . . . , 25 have a multiplicative inverse modulo 26?
5. (a) Check that that 2 is a multiplicative inverse for 3 modulo 5.

   (b) Carefully reread the second proposition in Section 1.5. use this proposition to find six other integers that are multiplicative inverses for 3 modulo 5.

6. Make sure you are familiar with the definitions and notation introduced in Section 1.6, especially for the following terms: congruence modulo a nonzero integer m, the integers modulo m, congruence/residue class.

7. Use a result in Section 1.6 (a proposition or corollary) to explain the following hand computation:

$$\big((24 + 17 * 11) * 3981\big)\%10 \;=\; (4 + 7)\%10 \;=\; 1$$

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

Name: ____

Read and take notes on Section 1.7, The Affine Cipher. The first main result in this section can be summarized as follows:

> **Proposition.** Let a and b be integers in the range $0, 1, \ldots 25$ with a relatively prime to 26 (guaranteeing the existence of a multiplicative inverse mod 26.) The affine cipher with key (a, b) can be described by the affine encryption function
>
> $$E_{a,b}(x) = (ax + b)\ \%26$$
>
> This function has an inverse, the decryption function with decryption key (c, d), given by the following formula:
>
> $$D_{a,b}(x) = (cx + d)\ \%26\,, \quad \text{where} \quad c = a^{-1} \ \text{ and } \ d = -a^{-1}b$$

Reading Questions

1. Look again at the example in the second paragraph, encrypting 'hello how are you.'

   (a) What is the key for this affine cipher? What is the affine encryption function?

   (b) Encode first word of the plaintext, 'hello,' using the assignment 'a' is 0, 'b' is 1, etc. This will give you the encoded plaintext for the first word, as a series of five numbers.

   (c) Encrypt the encoded plaintext using the affine cipher function $E_{3,11}(x)$, i.e. for each number in your code from **??**, multiply by 3, add 11, and reduce modulo 26.

(d) Decode the ciphertext using the assignment 0 is ‘A’, 1 is ‘B,’ etc. You should get the first word of the ciphertext given in the example, ‘GXSSB.’

(e) According to the proposition, the decryption function is $D_{3,11}(x) = (cx + d)$ %26, where c is the inverse of 3 mod 26 and d is $-11c$ %26. Check that $c = 9$ and $d = 5$.

(f) Decrypt your encoded ciphertext (the list of numbers from **??**) by applying the function $D_{3,11}(x) = (9x + 5)$ %26 to each number. You should recover the encoded plaintext from **??**.

2. (a) Why is a brute-force ciphertext-only attack harder for the affine cipher than for the shift cipher?

   (b) What kind of attack is likely to succeed against an affine cipher?

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

Math 316, 6.2, 6.3 The Euclidean Algorithm, Computing Inverses mod m

Name: ____

Read and take Section 6.2, The Euclidean Algorithm and skim through Section 6.3, Computing Inverses.

Reading Questions

1. The Euclidean Algorithm allows us to find the gcd of two numbers while avoiding what? Why is this desirable?

2. Use the Euclidean Algorithm to find the gcd of 58 and 63.

3. Run the Euclidean Algorithm backwards to find integers s and t such that $58s + 63t = 1$.

4. Give a multiplicative inverse for 58 modulo 63.

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

Math 316, 2.1 Counting, 2.2A Basic Ideas in Probability

Name: ______________________________

Read and take notes on Section 2.1, Counting and the beginning of Section 2.2, Basic Ideas: read up to but not including the last paragraph on page 26, which starts a discussion about picking colored balls out of an urn.

Reading Questions

1. Two mathematical quantities occur repeatedly in the counting examples in Section 2.1: *factorial* and *binomial coefficient*. Make sure you know the notation and formula for each.

2. Try exercises 2.1.01, 2.1.02, 2.1.03, 2.1.04.

3. Try exercises 2.1.05 and 2.1.06.

4. Try exercises 2.2.01 and 2.2.02.

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

Name: ______________________________

Finish reading and taking notes on Section 2.2, Basic Ideas.

Reading Questions

1. Make sure you understand the meanings of the following terms: sample space, trial, event, probability, compound event, mutually disjoint/exclusive events, independent trials, conditional probability.

2. There are two propositions in this section. Focus on understanding the *statements* of these propositions rather than the *proofs*.

3. True or false, with reasons. Let A and B be events.

   (a) The probability of A *and* B is $P(A \cup B)$.

   (b) The probability of A *or* B is $P(A) + P(B)$.

   (c) The probability of B, given that A has occured is $P(A \cap B)/P(A)$.

4. Try exercise 2.2.06.

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

Math 316, 2.3, 2.4 Statistics of English, Attack on the Affine Cipher

Name: ____

Read and take notes on Sections 2.3 and 2.4, Statistics of English and Attack on the Affine Cipher.

Reading Questions

1. From a cryptology perspective, what are the two uses for studying characteristics of English plaintext?

2. Which letters of the alphabet seem to account for over 50% of the letters appearing in English plaintext? What appears to be the most common word?

3. Give two reasons why ciphertext is easier to decrypt if blanks have not been eliminated.

4. Explain how knowledge of character frequency can be used to crack the affine cipher.

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

Math 316, 4.1 The Vigenère Cipher

Name: ____

Read and take notes on Section 4.1 The Vigenère Cipher.

Reading Questions

1. Encrypt ‘snowy day’ with the Vigenère cipher with key ‘cold.’

2. Known-plaintext attack: Suppose you know that the plaintext ‘drink your ovaltine’ has been encrypted via a Vigenère cipher with unknown key as ‘URTCR GSLR ZKHTXZNP’. Find the key and use it to decrypt the following ciphertext, ‘Z PCTMMV R MTARALRKP’.

3. Compare and contrast the Vigenère cipher and the one-time pad. What features do they have in common? What makes them different? What is the weakness of the Vigenére cipher?

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

Name: ______________________________

Read and take notes on Section 4.4 Expected Values.

Reading Questions

1. Make sure you understand the meaning of the following terms: random variable, expected value, fair wager, independent random variables and that you are familiar with the properties of expected value described in the propositions.

2. Let X and Y be random variables and c a real constant. Then

   (a) $E(X+Y) \;=$

   (b) $E(cX) \;=$

   (c) For X and Y to be independent means:

   (d) If X and Y are independent, then $E(XY) \;=$

3. Suppose Paul offers you the following wager. You roll a die, and if the result is an even number, he will pay you $2. If, however, the result is an odd number, you must pay him one dollar for each pip (dot) showing. (So for example, if you roll a one, you pay him $1.) Is this a fair wager? If not, are the odds in your favor or his?

4. Suppose there are 4 red balls and 6 blue balls in an urn, and we want to know the expected number of red balls to be drawn in 5 trials (replacing whatever ball is drawn in each trial.)

   Let Ω be the set of all possible outcomes of 5 trials. Let X be the random variable given by

   $$X(\omega) \ = \ \text{the number of red balls drawn in event } \omega$$

   We will break X down into the sum of simpler random variables.

   (a) Let X_1 be the random variable given by:

   $$X_1(\omega) \quad = \quad \begin{cases} 0 & \text{if the first ball drawn in } \omega \text{ is black} \\ 1 & \text{if the first ball drawn in } \omega \text{ is red} \end{cases}$$

   for ω an outcome in Ω. For example, if ω is the event RBRBB, then $X_1(\omega) = 1$. What is $E(X_1)$?

   Similarly define X_2 to tell whether or not the *second* ball drawn is black (0) or red (1), X_3 to tell whether the *third* ball drawn is black or red, etc., up to X_5.

   For example, if ω is the event RBRBB, then

   $$X_1(\omega) = 1, \ \ X_2(\omega) = 0, \ \ X_3(\omega) = 1, \ \ X_4(\omega) = 0, \ \ X_5(\omega) = 0$$

   What is $E(X_i)$, for $1 \leq i \leq 5$?

   (b) Notice that the number of red balls drawn in ω is

   $$X(\omega) \ = \ X_1(\omega) + X_2(\omega) + X_3(\omega) + X_4(\omega) + X_5(\omega)$$

   Use the additive property of expected value to find $E(X)$.

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

Name: ____

Read and take notes on the beginning of Section 4.5, Friedman Attack, up to and including the proposition on page 62. Concentrate on the the part up to and including the first proposition (page 59).

Note. A **substitution cipher**, as defined in Section 3.1, which we skipped, is a cipher for which "the encrypted form of a character of the plaintext occurs in the same location as the plaintext character." The shift cipher, OTP, affine cipher, and Vigenère cipher are all substitution ciphers.

Note. This section refers to the Kasiski attack several times. This is an attack on the Vigenère cipher that, when successful, reveals the length of the key, but not the key itself. Read Section 4.2, if you are interested to see how it works. You do not need to understand the Kasiski attack to understand the Friedman attack.

Reading Questions

1. (a) What is the formula for index of coincidence of two character streams y and z of the same length? (Make sure to include the formula for the auxiliary function δ.)

   (b) If two character streams are identical, what is their index of coincidence?

   (c) If two character streams are completely random, what would we expect their index of coincidence to be?

   (d) If two character streams have the frequency distributions of typical English, what would we expect their index of coincidence to be?

   (e) If two character streams with the frequency distributions of typical English have been encrypted with a substitution cipher, what would we expect their index of coincidence to be?

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

Name: ______________________________

Finish reading and taking notes on Section 4.5 Friedman Attack, starting at the middle of page 62, after the proof of the proposition.

Reading Questions

Suppose that a ciphertext y is encrypted by a periodic substitution cipher (a Vigenère cipher) with key $k = (k_0, k_1, k_2, \ldots, k_{m-1})$.

1. The attack on begins with finding the key length m (the period of the cipher). Let $y^{(+\ell)}$ be the ciphertext stream shifted forward by ℓ.

   (a) If the period m divides ℓ, what do we expect the index of coincidence of y and $y^{(+\ell)}$ to be?

   (b) If the period m does not divide ℓ, what do we expect the index of coincidence of y and $y^{(+\ell)}$ to be?

   (c) Look again at the example on page 64. For which shifts are the indices of coincidence higher than 0.05? (Note that the table lists the index times 100.) Write down the shift and the index of coincidence for each shift. Why is it reasonable to conclude that the shift is 13?

2. After having found the key length, the next step in the attack is to determine the differences between numbers k_i and k_j in the key.

   (a) Reread the first three paragraphs on page 66 (which begin “Next, . . . ”, “We take ‘slices’ . . . ”, and “In particular, . . . ”).

   (b) To determine the difference $k_i - k_j$ we look for a number t between 0 and 25 such that the index of coincidence of *what two character streams* is high enough?

3. After having found enough of differences $k_i - k_j$ in the numbers in the key, we can write the key in terms of a single unknown parameter, say k_0. How do we finish the attack? (See page 69.)

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

Math 316, 7.1, 7.2 Trapdoors and The RSA Cipher

Name: ________________________________

Read and take notes on the introduction to Chapter 7, Section 7.1 Trapdoors, and 7.2 The RSA Cipher. In Section 7.2, focus on the first few pages, up to and including the first three paragraphs of page 98 (before the part about the speed of encryption/decryption algorithms.)

Reading Questions

1. Explain why using asymmetric ciphers greatly reduces the number of keys required to maintain a communications network.

2. Explain how an asymmetric cipher and a symmetric cipher work together in practice, through use of a session key.

3. What is the trapdoor for the RSA cipher?

4. What does Euler's theorem say? Make sure to include a description of Euler's φ-function.

5. To understand the set-up of the RSA cipher, we will walk through a very simple example.

   (a) Choose primes $p = 7$, $q = 19$. (In practice, these should be large primes.) Are these numbers public or private?

   (b) The RSA modulus n is $n = pq$. What is n in our example? Is this number public or private?

   (c) What is $\varphi(n)$, in our example?

(d) What must be true about the encryption key e and the decryption key d for the decryption step to really decrypt? Which is public and which is private?

(e) Let $e = 5$. Show that choosing $d = 65$ will work.

(f) For $x = 6$, show that $D_{n,d}(E_{n,e}(x)) = x$. Feel free to use *Mathematica* for the modular arithmetic. The command `Mod[a,b]` computes $a \,\%\, b$.

6. Why is it important that exponentiation be 'easy' relative to factorization?

7. Why is it important that primality testing is 'easy' relative to factorization?

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

Name: ______________________________

Read and take notes on Sections 9.5: Exponentiation Algorithm.

Reading Questions

1. (a) How many steps (maximum) should it take to compute $2^{56} \,\%\, 10$ using the fast exponentiation algorithm?

   (b) Compute $2^{56} \,\%\, 10$ by hand, using the fast exponentiation algorithm.

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

Math 316, 7.3, 7.4 Primitive Roots, Discrete Logs, Diffie-Hellman Key Exchange

Name: ____

Read and take notes on 7.3 Primitive Roots, Discrete Logs and 7.4 Diffie-Hellman Key Exchange.

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 is the Diffie-Hellman Key Exchange? (It is not a cipher; it is a protocol. What does that mean? And what is it a protocol for?)

6. What is the "man-in-the-middle attack"?

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

Name: ____

Read and take notes on 7.5 ElGamal Cipher.

Reading Questions

1. What is the trapdoor for the ElGamal cipher?

2. Describe the public key (the numbers known to everyone) and the private decryption key (the number known only to the person who will decrypt messages) for the ElGamal cipher.

3. What is the private encryption key (the number known only to the person encrypting a message) for the ElGamal cipher?

4. What additional information needs to be sent, as a header, along with the ciphertext, in order for the decryptor to decrypt the ciphertext?

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

Math 316, 13.1, 13.2 Fermat Pseudoprimes, Non-Prime Pseudoprimes

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 316, 10.8 Euler's Criterion, 12.1-12.3 Quadratic Symbols

Name: ____

Read and take notes on Section 10.8, Euler's Criterion, focusing on the Corollary (Euler's Criterion), and Sections 12.1-12.3, Square Roots, Quadratic Symbols, and Multiplicative Property

Reading Questions

1. Make sure you know the statement of Euler's Criterion (as described in the Corollary in Section 10.8), the definitions of the quadratic (Legendre) symbol and the extended quadratic (Jacobi) symbol, and the multiplicative property of quadratic symbols.

2. Use Euler's Criterion to determine:

   (a) whether 2 is a square modulo 5.

   (b) whether 2 is a square modulo 101.

   (c) whether 14 is a square modulo 101.

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

   (a) $\left(\frac{2}{5}\right)_2$

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

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

4. Use the previous problem and either the definition of the Jacobi symbol or the multiplicative property of the Legendre symbol to evaluate the following:

   (a) $\left(\frac{2}{505}\right)_2$.

   (b) $\left(\frac{28}{101}\right)_2$.

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

Math 316, 12.4-12.5 Quadratic Reciprocity

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 316, 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 $b_1, b_2, \dots b_5$, 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 $b_6, b_7, \dots, b_{10}$, 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 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?

Math 316, 10.1-2, 14.1-2 Sun-Ze's Theorem, Basic Public Key Protocol and Secret-Sharing

Name: ____

Read and take notes on Sections 10.1 and 10.2 on Sun-Ze's Theorem and its application to solving systems of linear congruences. Focus on pages 140-141 in Section 10.2. Then read and take notes on the introduction to Chapter 14 Sketches of Protocols and Sections 14.1 and 14.2 Basic Public Key Protocol and Secret-Sharing. In Section 14.2, focus on the big ideas and not on the mathematical details of the secret-sharing model.

Reading Questions

1. Reread the example at the bottom of page 141.

   (a) Look back at RQ 6.2, 6.3 where we used the Euclidean algorithm to find integers s and t such that $58s + 63t = 1$. What are s and t?

   (b) Write the system of linear congruences

   $$\begin{cases} x \equiv 2 \mod 58 \\ x \equiv 3 \mod 63 \end{cases}$$

   as a single congruence using the trick near the top of page 141.

   (c) Describe the set of integers that are solutions to the system of linear congruences in (b).

2. Make sure you understand the following terms from the relevant parts of Chapter 14: passive and active eavesdroppers, passive and active cheaters, signature, man-in-the-middle attack, certificate authorities, timestamp, threshold scheme.

3. Describe the two flaws in the public-key set-up stemming from a lack of identity verification. What can be done to address these flaws?

4. Describe the active eavesdropping that a timestamp is meant to address.

5. In your own words, explain what a threshold scheme is.

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

Math 316, 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?

Math 316,   14.3, 14.3 Oblivious Transfer, Zero Knowledge Proofs

Name: ____

Read and take notes on Sections 14.3 and 14.4 Oblivious Transfer and Zero Knowledge Proofs.

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. Reread the description of a mathematical implementation of the more complicated version of oblivious transfer. In this case, what are the secrets? Why can't Bob find both of them?

4. Explain, in your own words, what a zero knowledge proof is.

5. Reread the description of the naive version of a zero knowledge proof. Suppose Peter knows the factorization $n = 659 \cdot 683$.

   (a) Vera chooses $x = 45\,632$ and computes $z = x^4 \,\%\, n$. What is z?

   (b) Peter computes the principal square roots y_1 and y_2 of z modulo 659 and 683, respectively. What are they?

   (c) Using Sun Ze's Theorem (and the Euclidean algorithm), Peter finds y such that $y = y_1$ mod 659 and $y = y_2$ mod 683. What is y?

   (d) Peter tells Vera y to convince her that he knows that factorization of n without divulging the factorization of n. Why is this convincing?

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

Name: ____

Read and take notes on the introduction to Chapter 16 Random Number Generators and Sections 16.1 Fake OTPs, 16.2 Period of a pRNG, 16.3 Congruential Generators.

Reading Questions

1. Make sure you understand the following terms: pseudo-random number generator, seed/key of a pRNG, keystream, periodic sequence, eventually periodic sequence, linear congruential generator

2. (a) Explain, in your own words, what a pseudo-random number generator is.

   (b) Name two pRNGs that are not good enough for cryptographic purposes and one that is.

3. Explain why the cryposystem described in Section 16.1 is a *fake* OTP as opposed to a genuine one.

4. Given the modulus $m = 300$, multiplier $a = 17$, and the seed $s_0 = 3$, list the first 25 numbers in the stream generated by the simplest linear congruential generator described in the second paragraph of Section 16.3. What is the period of this generator?

5. Given the modulus $m = 300$, multiplier $a = 17$, the integer $b = 67$, and the seed $s_0 = 3$, list the first 10 numbers in the stream generated by the linear congruential generator described in the third paragraph of Section 16.3. What is the period of this generator?

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

Name: ____________________

Read and take notes on the Section 16.4 Feedback Shift Generators.

Reading Questions

1. Make sure you understand what the coefficients and the seed/initial state of a feedback shift generator are.

2. Fix a size $N = 3$, a modulus $m = 2$, coefficients $c = (1, 0, 1)$, and a seed $s = (1, 1, 1)$.

   (a) Write the recursion relation as an equation $s_{n+1} = \dots$.

   (b) Define a matrix C that can be used to write the recursion relation as a matrix equation.

   (c) Write the recursion relation as a matrix equation, using the matrix C.

   (d) What is the keystream produced by this feedback shift generator? Include the first 12 terms.

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

Name: ______________________________

Read and take notes on the Section 16.6 Blum-Blum-Shub Generator.

Reading Questions

1. Let $p = 3$, $q = 7$, and $s_0 = 12$.
   (a) Compute the first five terms of the sequence s_i given by the recursive formula $s_{i+1} = s_i^2 \,\%\, pq$.

   (b) Compute the first five terms of the sequence b_i given by $b_i = s_i \,\%\, 2$.

2. Let $p = 7$, $q = 11$, and $s_0 = 8$.
   (a) Compute the first ten terms of the sequence s_i given by the recursive formula $s_{i+1} = s_i^2 \,\%\, pq$.

   (b) Compute the first ten terms of the sequence b_i given by $b_i = s_i \,\%\, 2$.

   (c) What is the period of this eventually periodic sequence?

3. Let $p = 5279$, $q = 7103$, and $s_0 = 27$. Given that $s_{i+1} = s_i^2 \,\%\, pq$ for $i \geq 0$, compute the first fifteen terms of the sequence b_i given by $b_i = s_i \,\%\, 2$.

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

Name: ____

Read and take notes on Sections 9.1: Fermat's Little Theorem, 9.2: Factoring Special Expressions, 9.3: Mersenne Numbers, and 9.4 More Examples.

Reading Questions

1. What kind of factorizations does Fermat's Little Theorem allow us to speed up?

2. (a) Consider $N = 3^{14} - 1 = 4\,782\,968$. According to the corollary in Section 9.2, we do not need to check *all* primes less than $\sqrt{N}$ to find the prime factors of N. Which primes should we check?

   (b) Factor N by hand, or at least without using anything more than a scientific calculator.

   (Hint: Start by factoring out as many 2s as possible. Then look at the conditions in (a). Also, take a look at the example in Section 9.4 on factoring $3^7 - 1$.)

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

Math 316, 18.1 Pollard's Rho Method

Name: ______________________________________

Read and take notes on the introduction to Chapter 18, Factorization Attacks, and Section 18.1, Pollard's Rho Method. **Note**: The function $f(x)$ given in the algorithm should include a reduction modulo n, as is made clear by the examples at the end of the section.

Reading Questions

1. Describe two advantages and two disadvantages of Pollard's rho method.

2. How does one initialize the algorithm for Pollard's rho method, i.e. what are x, $f(x)$, and y at the beginning of the algorithm? (See note above.)

3. Consider $n = 209$.

   (a) Use Fermat's Test (with base $b = 2$) to show that n is composite.

   (b) Apply one cycle of the algorithm of Pollard's rho method to n: compute $x - y$ and use the Euclidean algorithm to find g. Have you found a proper factor of n? Has the algorithm failed? If not, repeat the algorithm to find a proper factor of n.

4. Consider $n = 4031$.

   (a) Use Fermat's Test (base $b = 2$) to show that n is composite.

   (b) About how many cycles of the algorithm to we expect to need to find a factor of $n = 4031$?

   (c) Apply Pollard's rho method to $n = 4031$ to find a factor. (You may use *Mathematica* or some other tool to compute gcds.) How many cycles does it actually take to find a factor?

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

Name: ______________________________

Read and take notes on 18.2, Pollard's $p-1$ Method. **Note**: The change of base formula for logarithms is $\ln(x)/\ln(a) = \log_a(x)$. This fact is useful for understanding how the examples follow the given algorithm.

Reading Questions

1. Make sure you understand the meanings of the following terms: B-smooth, smoothness bound.
2. **Note.** For a set $\{p_1, \ldots, p_t\}$ of primes (usually consecutive primes, starting with 2), for a number to be $\{p_1, \ldots, p_t\}$-smooth means that all its prime factors lie in the set $\{p_1, \ldots, p_t\}$. If $\{p_1, \ldots, p_t\}$ is the set of primes less than or equal to a bound B, than being B-smooth is equivalent to being $\{p_1, \ldots, p_t\}$-smooth.
3. (a) In what cases does Pollard's $p-1$ method work well?

   (b) Why is this method is important, despite the fact that it only works in certain special cases?
4. Fix $B = 10$. Give three examples of numbers that are B-smooth and one example of a number that is *not* B-smooth.
5. Consider $n = 1581$. Fix $B = 3$.

   (a) First we choose random b in $1 < b < n$. Choose $b = 1000$. Then compute $g = \gcd(b, n)$. What is g? Explain why we must continue with the algorithm.

(b) The primes less than or equal to B are $p_1 = 2$ and $p_2 = 3$. For $p_1 = 2$:

i. Compute $\ell = \text{floor}(\ln(n)/\ln(p_1))$.
ii. Compute $r = p_1^{\ell}\ \%n$.
iii. Replace b by $b^r\ \%n$.
iv. Compute $g = \gcd(b-1, n)$.

(c) Explain why we may stop the algorithm at this point.

(d) If we had found $g = 1$ in the previous part, what would we have needed to do?

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

Name: ______________________________

Read and take notes on 18.3, Pocklington-Lehmer Criterion. Focus on Proth's Corollary, Fermat numbers, Pepin's Test, and Euler's lemma for speeding up the search for factors.

Reading Questions

1. Make sure you are familiar with the following: Proth's Corollary, Fermat numbers, Pepin's Test, Euler's speed-up Lemma, Mersenne numbers, the Lucas-Lehmer test.
2. (a) In what cases is the Pocklington-Lehmer criterion especially useful?

   (b) In what cases is it most often applied?

   (c) How else can the technique be used, besides being used to prove primality?
3. Let $N = 5$.

   (a) Write N in the form $N = u2^n + 1$, where $u < 2^n$ and u is odd.

   (b) Find b such that $b^{(N-1)/2} = -1 \bmod N$.

   (c) What does Proth's Corollary allow you to conclude about N?

4. Use Pepin's Test to show that the third Fermat number, $F_3 = 257$, is prime.

5. What lemma (due to Euler) allows us to speed up the search for prime factors of Fermat numbers by a factor of 128? State the lemma here.

6. Take a look at the following recent article. (The link is live in the pdf file.) What is the largest known prime number?

   http://www.nytimes.com/2016/01/22/science/new-biggest-prime-number-mersenne-primes.html?_r=0

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

Math 316, 8.1-8.3 Prime Numbers, 18.4 Strong Primes

Name: ____

Read and take notes on Sections 8.1, 8.2, 8.3: Euclid's Theorem, Prime Number Theorem, Primes in Sequences and 18.4: Strong Primes.

Reading Questions

1. (a) Who proved the Prime Number Theorem, and in what year?

   (b) What does the Prime Number Theorem say? (Make sure to explain what the symbol $\sim$ means.)

   (c) According to the Prime Number Theorem, about how many primes are there less than 1000?

2. (a) What does Dirichlet's theorem say in the cases $a = 4$, $b = 1$ and $a = 4$, $b = 3$?

   (b) About how many primes congruent to 1 mod 4 are there less than 1000?

   (c) About how many primes congruent to 3 mod 4 are there less than 1000?

3. (a) What is the heuristic version of the Prime Number Theorem used in the algorithm for strong primes? (This is at the very end of the section.)

   (b) What is the heuristic version of Dirichlet's theorem used in the algorithm for strong primes?

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

Name: ______________________________

Read and take notes on Section 18.5: Primality Certificates.

Reading Questions

1. Reread the first example in this section, which describes how to find a primality certificate for $N = 1\,000\,000\,033$.

   (a) Why do we have good reason to think this is a prime? More precisely, what is the probability that N is prime, given the test described at the beginning of the example?

   (b) Using trial division with small primes, we can write $N - 1$ as a product of small primes and another factor. In this example, "small" means less than or equal to 127. Write the resulting factorization of $N - 1$.

   (c) This allows us to write $N - 1 = K \cdot U$, where the prime factorization of K is known and, although the prime factorization of U is unknown, we do know that it has no prime factors less than a certain bound B. What are K, U, and B in this example?

   (d) To use the second version of the Lucas-Pocklington-Lehmer theorem, what do we need to verify about $B \cdot K$? (See the bulleted recap of the second version of the Lucas-Pocklington-Lehmer theorem, hereafter refered to as LPL v2, at the beginning of the section.) Verify that condition here.

   (e) For each prime q dividing K, we want to find b_q satisfying two criteria. What are the two criteria? (Again, see the bulleted recap of LPL v2.)

(f) List the primes q dividing K and the numbers b_q that are found to work in this example.

(g) The last bullet point in the recap of LPL v2 requires that we find a number b_0 satisfying two criteria. What are the two criteria?

(h) What number b_0 is found to work in this example?

(i) What is the data comprising the primality certificate for N in this example/

(j) Explain, in your own words, why providing the stated data is a primality certificate for N. (See the remark immediately following the statement of the primality certificate for this example.)

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

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 $x^2 = y^2 \bmod n$ but $x \neq \pm y \bmod n$.

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?

Name: ____

Read and take notes on Sections 19.1, Gaussian Elimination and 19.3, Dixon's Algorithm.

Reading Questions

1. Section 19.1 is a review of one of the basic algorithms in linear algebra: using row reduction to find a dependency relation among m vectors in an n-dimensional vectorspace, where $m > n$. Make sure you know the relevant terms: linear dependency relation, linear combination of vectors, etc.

2. From Section 19.3, make sure you understand what a factor base is and what it means for a number to be smooth with respect to a factor base.

3. In the very simplest cases, if we are lucky, Dixon's Algorithm can be significantly abbreviated, as follows:

   > We aim to factor a number n. We choose a factor base $S = \{p_1, \ldots, p_t\}$. We choose a number a and let $b = a^2 \,\%\, n$. Suppose we are *lucky* and b is both smooth with respect to S and a square in $\mathbb{Z}$. In this case let $x = a$ and $y = \sqrt{b}$ (the square root of b in $\mathbb{Z}$.) Then $x^2 = y^2 \bmod n$, and, if we are again lucky, $x \neq \pm y$, in which case $\gcd(x \pm y, n)$ are proper factors of n.

   Use this simple version of Dixon's Algorithm with factor base $\{2, 3\}$ to factor n, for

   (a) $n = 323$, with lucky choice $a = 18$.

   (b) $n = 1147$, with lucky choice $a = 34$.

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

Name: ______________________________

Read and take notes on Section 19.4, Non-Sieving Quadratic Sieve. Section 19.4 describes various issues with and improvement to Dixon's Algorithm and includes several examples.

Reading Questions

1. What two parts of Dixon's Algorithm are optimized/improved in this section? (See the first paragraph.)

2. What advantages are there to choosing a's that are close to the square root of n? (There are two! One is mentioned in the first remark, the other mentioned immediately before the last example.)

3. How should the factor base be modified if the b's are computed in such a way that they may be negative?

4. What is the advantage to having a larger factor base? What is the disadvantage?

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

Name: ______________________________

Read and take notes on Section 19.5, Continued Fractions Sieve.

Reading Questions

1. What part of Dixon's Algorithm is optimized/improved in this section?

2. Find a series of rational approximations for $\sqrt{2}$ using continued fractions, as follows:
   (a) Let $x_0 = \sqrt{2}$. Find $a_0 = \text{floor}(x_0)$. Then $r_0 = a_0$.
   (b) Find $x_1 = \frac{1}{x_0 - a_0}$ and $a_1 = \text{floor}(x_1)$.
   (c) Find $r_1 = \frac{p_1}{q_1} = a_0 + \frac{1}{a_1}$.
   (d) Find $x_2 = \frac{1}{x_1 - a_1}$ and $a_2 = \text{floor}(x_2)$.
   (e) Find $r_2 = \frac{p_2}{q_2} = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}$.
   (f) Find $x_3 = \frac{1}{x_2 - a_2}$ and $a_3 = \text{floor}(x_3)$.
   (g) Find $r_3 = \frac{p_3}{q_3} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}}$.

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