CS 70 Discrete Mathematics and Probability Theory
Spring 2018 Ayazifar and Rao Midterm 2

PRINT Your Name: _____, _____
(last) (first)

SIGN Your Name: _____

PRINT Your Student ID: _____

WRITE THE NAME OF your exam room: _____

Name of the person sitting to your left: _____

Name of the person sitting to your right: _____

- After the exam starts, please *write your student ID (or name) on every odd page* (we will remove the staple when scanning your exam).
- We will not grade anything outside of the space provided for a problem unless we are clearly told in the space provided for the question to look elsewhere.
- The questions vary in difficulty, so if you get stuck on any question, it might help to leave it and try another one.
- **No justifications are needed for True/False or Short Answer questions. Make sure you bubble in or write your answer in the provided box, accordingly. Work outside the box may be considered for partial credit where tricky calculations are involved.**
- You may consult only *2 sheets of notes*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- There are **12** single sided pages on the exam. Notify a proctor immediately if a page is missing.
- **You may, without proof, use theorems and lemmas that were proven in the notes and/or in lecture.**
- **You have 120 minutes: there are 6 questions with a total of 59 parts on this exam worth a total of 165 points.**

Do not turn this page until your instructor tells you to do so.

1. True/False. 2 points/part. 14 parts. No partial credit. No work necessary. Fill in bubbles.

1. The equation $7x = y \pmod{10}$ has a solution x for every value y.

   ◯ True

   ◯ False

2. The function $f(x) = ax \pmod{N}$ is always a bijection if $gcd(a,N) = 1$.

   ◯ True

   ◯ False

3. If there are k numbers that are relatively prime to N in $\{0,\ldots,N-1\}$, then $a^k = 1 \pmod{N}$ if $gcd(a,N) = 1$.

   ◯ True

   ◯ False

4. For all $n > 2$, there is at least one element of $\{2,3,\ldots,n-1\}$ with a multiplicative inverse $\pmod{n}$.

   ◯ True

   ◯ False

5. It is possible to measure out exactly 1 oz. of water using only cups of size 56 oz. and 14 oz.

   ◯ True

   ◯ False

6. A polynomial, $P(x)$, modulo a prime, p, of degree exactly d (that is, the coefficient of x^d is non-zero), where $d < p$, must have at least d roots.

   ◯ True

   ◯ False

7. If two degree d polynomials intersect on $d+1$ points, they must be the same polynomial.

   ◯ True

   ◯ False

8. There is no program that takes a program P, an input x, and an integer k and determines if it halts in k^k steps on input x.

   ◯ True

   ◯ False

9. For any countable subset, S, of the reals, $\mathbb{R}$, we have $\exists \varepsilon > 0 \in \mathbb{R}, \forall x,y \in S, (x \neq y) \implies (|x-y| \geq \varepsilon)$.

   ◯ True

   ◯ False

10. We define the output of a program as the string it prints (possibly infinite length) when given a finite length input. Then, the set of outputs of any particular deterministic program is countable.

◯ True

◯ False

11. For events $A, B, C \subseteq \Omega$, we have $Pr[(A \cap B) \cup C] \geq Pr[A \cup C]$.

◯ True

◯ False

12. If events A, B and C are mutually independent, so are $\bar{A} \cap B$ and C.

◯ True

◯ False

13. For any events A and B, $Pr[A|B] + Pr[A|\bar{B}] = Pr[A]$.

◯ True

◯ False

14. For events A and B, if $Pr[A|B] > Pr[A]$ then $Pr[A|\bar{B}] < Pr[A]$.

◯ True

◯ False

2. Short Answer/Proof: Modular Arithmetic to RSA. 3 points/part. 15 parts.

Put your answers in boxes where provided. Answers outside the box will not be graded.

1. What is $\gcd(0,n)$?

2. What are the possible values of $\gcd(n,n+2)$?

3. For x,y with $gcd(x,y)=d$, where $ax+by=d$, and $zx=kd \pmod{y}$. What is z? **The answer may be in terms of a,b,k,x,y and/or d.**

4. What is the smallest possible positive value of the expression $14x \pmod{21}$ in $\{1,\ldots,20\}$?

5. What is $7^{11} \pmod{15}$?

6. Find $x \pmod{90}$ where $x = 1 \pmod{9}$ and $x = 3 \pmod{10}$.

7. How many numbers in $\{0,\ldots,34\}$ are relatively prime to 35.

8. What are the last two digits of 9999^9?

9. For a prime p, how many roots does the polynomial $x^{p-1}-1 \pmod{p}$ have?

10. What is the (simplified) result of multiplying out the polynomial $(x-1)(x-2)\cdots(x-p+1) \pmod{p}$, where p is a prime?

11. Suppose we want to send a length n message, but the channel can introduce p erasure errors and q general errors. How long should the message we send through the channel be, in order to guarantee that the the other side can decode it successfully?

12. Recall that RSA computes $y^d \pmod N$ where $N = pq$ for p and q being prime.

    (a) If p and q have n-bits, how many bits does it take to represent $N = pq$? (Any answer within 1 or 2 bits of the right answer gets full credit.)

    (b) Consider $y = a \pmod p$, we know that $y^d = a^d \pmod p$. Prove that $y^d = a^u \pmod p$ where $u = d \pmod{p-1}$.

    (c) L $y = a \pmod p$ and $y = b \pmod q$. Give an expression for $y^d \pmod{pq}$ in terms of $m_1 = a^u \pmod p$ and $m_2 = b^v \pmod q$, where $u = d \pmod{p-1}$ and $v = d \pmod{q-1}$.

13. Alice is selling books for \$10. She sets up an RSA scheme with public key (N, e) and private key d. People buy her book by encrypting their credit card number x as $c = x^e \pmod N$ and sending c through a public channel to Alice, who then charges \$10 to the decrypted credit card number c^d. If Eve can listen in on the channel, how could she take advantage of this setup?

3. Short Answer: Polynomials. 3 points/part. 5 parts.

Put your answers in boxes where provided. Answers outside the box will not be graded.

For the following, recall that a polynomial, $P(x)$, contains a point (a,b) when $P(a) = b$. And two polynomials, $P(x)$ and $Q(x)$, intersect at a point (a,b) when $P(a) = Q(a) = b$.

1. Given two polynomials $P(x)$ and $Q(x)$ of degrees d_1 and d_2 respectively, consider $R(x) = P(x)Q(x)$. We claim that we can recover $P(x)$ and $Q(x)$ with any r points on $R(x)$ and any q points on $Q(x)$, What are r and q? (You should give the minimum possible values for r and q here.)

2. Recall the secret sharing scheme where the secret is $P(0)$. What is the secret corresponding to a polynomial of degree at most 2 where $P(1) = 3 \pmod 5$ and $P(2) = 1 \pmod 5$ and $P(3) = 4 \pmod 5$?

3. Consider sending an n packet message where each packet has b-bits, and we want to encode the message so that k packets can be lost using our polynomial encoding scheme modulo a prime p. How large is p required to be in this setup?

4. What is the maximum number of points at which two distinct degree d polynomials can intersect?

5. For a prime p, and $d < p$, how many polynomials in $GF(p)$ (modulo arithmetic modulo p) of degree d are there with exactly d roots? (Here, we assume $(x-2)^2$ has *two roots* at $x = 2$.)

4. Short Answer: Counting. 3 points/part. 9 parts. Answers should be in boxes.

1. How many permutations of the letters in "STANFORD=BORING" are there? (Hint: there are 15 letters total, and one permutation is: "ABDFGINNOORRST=".)

2. We have a classroom of n people, who are playing a (sort of) tournament of rock paper scissors. At every turn, one pair of students is picked from the pool of students who are still in the game, to play in front of the class. The player who loses the game is out, and the player who wins is put back in the pool. How many different possible ways are there for this tournament to play out?

3. How many ways are there to divide up nine distinguishable people into three indistinguishable teams of three?

4. Consider the set $S = \{0,1,2,3,4,5,6,7,8,9\}$. We wish to count the number of distinct 3-element subsets of S where the sum of the elements in the subset is divisible by 3.

   (a) Case 1: How many 3-element subsets of S have one element which is equivalent to $1 \pmod 3$, one which is equivalent to $2 \pmod 3$ and one which is equivalent $0 \pmod 3$?

   (b) Case 2: How many 3-element subsets of S have all the elements being equivalent $\pmod 3$?

5. We wish to count how many undirected graphs on six vertices there are, where every vertex has equal degree.

   (a) How many such graphs are there such that all vertices have degree one?

   (b) How many ways can we form two disjoint cycles of length three with six vertices?

   (c) How many ways can we form a long cycle of length six?

   (d) How many graphs are there where all vertices has equal degree? (For partial credit, express your answer in terms of a, b, c, the answers to the previous parts. For full credit, you must have the numerical answer.)

5. Counting/Combinatorial Proof. Points by part: 2/5/4. Put your answers in boxes where provided otherwise use the space provided.

1. Recall that a subset S of n elements of size k is uniquely specified by the $n-k$ items left out of S. Write a combinatorial identity that corrsponds to this statement.

2. Use a combinatorial argument to prove that $\binom{n+m}{k} = \sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i}$

3. Consider the following $\sum_{k=0}^{n} k^2 \binom{n}{k} = n(n-1)2^{n-2} + X$. Give an expression for X (in terms of n only.)

6. Probability. 3 points/part. 13 parts.

Answers in boxes. Calculations outside may be considered for partial credit.

For this problem, recall Dice have six sides.

1. Given $Pr[A|B] = 1/3$, $Pr[B] = 1/2$, what is $Pr[A \cap B]$?

2. Given $Pr[A|B] = 1/3$, $Pr[B] = 1/2$ and $Pr[A|\bar{B}] = 1/2$, what is $Pr[B|A]$?

3. Suppose, we choose a permutation of $1, \ldots, 100$ where each permutation is equally likely. What is the probability that we get a permutation where 1, 2, and 3 are in order but not necessarily adjacent.

4. What is the size of the sample space for rolling four distinguishable dice?

5. You roll a fair die 4 times. What is the probability that the first time you get a six is on the fourth roll?

6. You roll a fair die 4 times. What is the probability that the second time you get a six is on the fourth roll?

7. A sequence of dice rolls is considered "lucky" if there exists two consecutive rolls of the same number. What is the probability that a sequence of 4 dice rolls is "lucky"?

8. There 2 dice in a bag. One die is cheating in that it has two sixes which are on opposite faces (which means there is no side with 1 pip on it). The other die is a fair six sided die. You close your eyes, reach into the bag and choose one of the dice to roll.

   (a) What is the probability that you get a six on the first roll?

   (b) You get a six on the first roll. What is the conditional probability that you chose a cheating die?

   (c) Now you roll the same die again (this is the second roll). What is the probability that you roll a six again? **(For partial credit, you may express your answer in terms of b, the answers to part (b).**

   (d) On the second roll you get a six. What is the conditional probability that you chose the cheating die? **(For partial credit, you may express your answer in terms of b, c, the answers to part (b) and (c).**

9. Consider choosing k pairs of people from n people, allowing for repetition within a pair. That is, to create each pair, we choose from all n people twice.

   (a) What is the probability that we choose the same person twice in the first pair?

   (b) Upper bound the probability that the same person is chosen twice in any of the k pairs using the union bound. (Answer is expression involving k and n.)