CS 70 Discrete Mathematics and Probability Theory
Spring 2019 Ayazifar and Rao Midterm 2

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

SIGN Your Name: _____

PRINT Your Student ID: _____

PRINT 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.

- The questions **vary in difficulty**, so if you get stuck on any question, it might help to leave it and try another one.
- If there is a box provided, put your answer in it. If not, use the space provided for your proof or argument.

- You may consult only *two 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 **15** single sided pages including the cover sheet 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 11 questions (with 51 parts) on this exam worth a total of 161 points.**
- Graphs are simple and undirected unless we say otherwise.

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

SID:

1. TRUE or FALSE? 2 points each

For each of the questions below, answer TRUE or FALSE. No need to justify answer.

Please fill in the appropriate bubble!

1. If the set of prime numbers that divide x is the same as the set of prime numbers that divide y, then $x = y$.

   ◯ True

   ◯ False

2. For primes p and q, the function $f(x) = x^{k(p-1)(q-1)+1} \pmod{pq}$ is a bijection for all integers k.

   ◯ True

   ◯ False

3. Every degree exactly d polynomial over $GF(p)$ can be factored into d polynomials of degree 1, for all d and all primes p.

   ◯ True

   ◯ False

4. Let a "probability problem" be a math problem written in LaTeX for which the answer is a probability. There exists a bijection between the set of probability problems and the interval $[0,1]$.

   ◯ True

   ◯ False

5. Given events A and B in a probability space, the events are independent if and only if $A \cap B$ is empty.

   ◯ True

   ◯ False

6. Suppose we flip 3 fair coins, let A be the event that all the flips are the same and let B be the event that there are more heads than tails. The events A and B are independent.

   ◯ True

   ◯ False

7. A, B and C being pairwise independent implies that A, B and C are mutually independent.

   ◯ True

   ◯ False

2. Short Answer: RSA. 3 points each.

Write your answer in the simplest form possible. You should use only the variables in the question unless otherwise specified.

1. Given an RSA scheme with public key, (N, e), and the encryptions $E(x) = x'$ and $E(y) = y'$, what is the encryption of xy? (It should be a function of x', y', e, N. You are not given x or y.)

2. What is $[8(7^{-1} \pmod 5)(7) + 6(5^{-1} \pmod 7)(5)] \pmod 5$? (Answer should be in simplest terms.)

3. Let $f(x) = x^7 \pmod{143 = 11 \cdot 13}$, where $f : \{0,1,2,\ldots,142\} \to \{0,1,2,\ldots,142\}$. What is the size of the range of f?

4. Let Bob have a public key of $(N, e) = (77, 13)$. What is his corresponding private key d?

5. For a natural number $n \geq 1$, if $a^7 = 3 \pmod n$ and $a^2 = 4 \pmod n$, what is $a^{11} \pmod n$?

6. For primes p and q, what is the probability that a random element of $\{0,\ldots,pq-1\}$ is a multiple of p or q?

3. Polynomials++: Short Answer. 3 points each.

Write your answer in the simplest form possible. You should use only the variables in the question unless otherwise specified.

1. Consider that $P(x) = 3x^2 + a_1x + s \pmod 5$ encodes a secret s as $P(0)$; given $P(1) = 3$, $P(2) = 4$, what is the secret?

2. Given polynomial $P(x)$ of degree d with r_P roots and $E(x)$ of degree k with r_E roots, what is the maximum number of roots that $Q(x) = P(x)E(x)$ can have? (Assume $P(x)$, $E(x)$ are over reals.)

3. Given a polynomial $P(x)$ and 7 ordered pairs $(x_1, r_1), \ldots, (x_7, r_7)$ where $r_i = P(x_i)$ except for at x_1 and x_5. That is, $P(x_1) \neq r_1$ and $P(x_5) \neq r_5$. What is the error locator polynomial in the Berlekamp-Welch algorithm?

In this problem, we will be working with polynomials over $GF(p)$ where p is a prime, unless otherwise specified. Furthermore, when we say we pick a polynomial of degree at most k at random, we pick $P(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0$ where a_i are chosen uniformly at random from $\{0, \ldots, p-1\}$.

4. Assuming $k < p$, how many degree at most k polynomials are there over $GF(p)$?

5. Given 2 distinct values x_1 and $x_2 \pmod p$, we pick a polynomial $P(x)$ of degree at most 3 at random. What's the probability that $P(x_1) = P(x_2) \pmod p$?

6. Now suppose you have five distinct values x_1, x_2, x_3, x_4, x_5, and $P(x)$ is again a polynomial of degree at most 3 chosen at random. What is the probability that $P(x_1) = P(x_2) = P(x_3) = P(x_4) = P(x_5)$? (Careful.)

7. How many polynomials of degree at most 5 in $GF(p)$ have **exactly** 5 fixed points? (A fixed point for $P(x)$ is a value a where $P(a) = a$. Assume $p \geq 6$.)

8. Let $P(x)$ be a degree exactly 4 polynomial with a leading coefficient of 1 and fixed points at $1, 2, 3$ and 4. What is $P(5)$? (Hint: consider $P(x) - x$.)

9. What is the probability that a randomly chosen polynomial modulo a prime p of degree at most d has exactly d distinct roots? (Assume $p > d$.)

4. Countability. 5 points each part.

We say a set $A \subseteq \mathbb{Q}$ is *downward closed* if, for each $x \in A$, every rational number smaller than x is also in A. Let $D_{\mathbb{Q}}$ be the set of all downward closed subsets of $\mathbb{Q}$ and let $D^L_{\mathbb{Q}}$ be the set of all downward closed subsets of $\mathbb{Q}$ *that have a largest element*.

For example, the set S of all rationals less than $\sqrt{2}$ is downward closed. It is, however, not in $D^L_{\mathbb{Q}}$ as S does not have a largest element.

1. Prove that $D^L_{\mathbb{Q}}$ is countably infinite. *(Hint: find a bijection $b : D^L_{\mathbb{Q}} \to \mathbb{Q}$)*

2. Prove that $D_{\mathbb{Q}}$ is uncountable. *(Hint: find a one-to-one function $f : \mathbb{R} \to D_{\mathbb{Q}}$. You may use without proof the fact that for any $x, y \in \mathbb{R}$ with $x < y$, there exists a $q \in \mathbb{Q}$ such that $x < q < y$.)*

5. Computability *I love CS70*. 6 points

The program `Test70(P)` takes in another program `P` as input and determines whether the program `P` returns "I love CS70" on exactly 70 inputs. That is, `Test70(P)` will return true if `P` returns "I love CS70" on 70 different inputs, and does not return it for all other inputs. Otherwise, `Test70(P)` returns False. Show that `Test70(P)` cannot exist.

6. Counting. 3 points each.

Please state your answer in the simplest form possible. Complicated sums are not necessary for this problem.

1. An outfit consists of a shirt, hat, and skirt where each comes in three colors: blue, gold, and white. How many outfits are there where items are not all the same color? In particular, one can wear a blue shirt, gold hat, and a gold skirt, but one cannot wear all gold clothes.

2. How many permutations of the numbers 1 through n are there?

3. How many permutations of the numbers 1 through n are there such that 1 comes before 2 and after 3? Assume $n > 3$.

For each permutation σ of 1 through n, let $\sigma(i)$ denote the value at position i. For example, if the permutation is $2,4,1,3$, we have $\sigma(1) = 2$ and $\sigma(2) = 4$.

4. For a fixed $1 \leq k \leq n$, how many permutations σ of 1 through n are there where for all $i < k$, $\sigma(i) < \sigma(k)$? Express your answers in terms of n and k.

5. How many permutations of 1 through n are there such that for each i, $\sigma(\sigma(i)) = i$ and $\sigma(i) \neq i$? (For example, the permutation $3,4,1,2$ is such a permutation, since for example $\sigma(\sigma(1)) = \sigma(3) = 1$. You may assume n is even.)

7. Combinatorial Proof. 8 points.

Prove the following combinatorial identity using a combinatorial proof:

$$\sum_{k=2}^{n-5} \binom{k}{2} \binom{n-k}{5} = \binom{n+1}{8}$$

(Hint: Consider selecting 8 elements from $\{1, \ldots, n+1\}$.)

8. Probability (and counting): Short Answer. 3 points each.

1. For the probability space consisting of rolling two six-sided dice, the event A that the dice add up to 3 is $\{(1,2),(2,1)\}$. What is the event that the dice sum to 5?

2. When rolling two six sided dice, what is the probability that the dice sum to 5?

3. Consider rolling a six-sided die 5 times, what is the probability that you see a 2 exactly twice? (An expression here is fine, no need to simplify.)

4. For events A and B, where $Pr[A \cup B] = .6$ and $Pr[A \cap B] = .2$, what is $Pr[A] + Pr[\overline{B}]$?

5. For events A and B, where $Pr[A|B] = .4$, $Pr[A|\overline{B}] = .8$, and $Pr[B] = .25$, what is $Pr[A]$?

6. Given that you toss two coins with heads probabilities p and q, what the probability that both are heads? (Assume they are indendependent coins.)

7. Consider two coins with heads probability $1/3$ (coin A) and $2/3$ (coin B). If the coins are tossed in random order, and the result is heads and then tails (i.e., the outcome is 'HT'), what is the probability that the coin A was tossed first? Answer as a simplified fraction. (Note that it is going to be less than $1/2$.)

8. For an event A with non-zero probability what is $Pr[A]$ if A is independent of itself?

9. You have 5 black cards and 5 red cards. You shuffle thoroughly and draw five of them. What's the probability that the black cards are consecutive and red cards are consecutive? Examples that satisfy the condition are RRRRR, BBRRR, and RRRRB. However, RBRRR and BBBRB do not satisfy the condition. Express your answer as a simplified fraction.

10. Jonathan, Jerry, and Bob are deciding which of the four courses, 61A, 61B, 61C, and 70, to enroll in next semester. They want to sign up for the courses such that no course is taken by all three. However, for each pair of people, there should be at least one course that they take together. How many ways can they sign up for the courses, (ignoring pre-requisites)? Note that it is possible for some class to not be taken by any of the three. Answer as a single positive integer. The chart below shows an example enrollment that satisfies the conditions.

	61A	61B	61C	70
Jonathan	Y	N	Y	Y
Jerry	N	Y	N	Y
Bob	Y	Y	N	N

9. Probability: Quick Argument. 4 points.

1. **[Complementary Independence]**
   Prove—in a succinct, yet clear and convincing fashion—that the following assertion is true:

   If events A and B are independent, then so are the events A and B^c, where B^c denotes the complement of B.

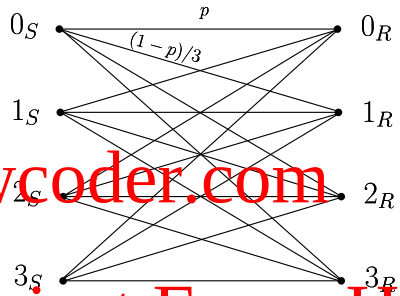
Nothing written below will be considered in evaluating your work. You're limited to the space given above.

10. [Digital Communication Errors]. 3 points each.

In each tick of a system clock, a digital communication transmitter is *equally likely* to transmit only a 0, a 1, a 2, or a 3. That is, we have $P[i_S] = 1/4$ for all i_S.

The communication channel is prone to error, so the number the transmitter sends is not necessarily what arrives at the receiver (shown on the right side of the diagram). With probability p, each number that is sent is received intact (without error), and with probability $1-p$ is corrupted into the other numbers with *equal likelihood*. Specifically, for all $i, j \in \{0,1,2,3\}$, we have

$$Pr[j_R|i_S] = \begin{cases} p & \text{if } i = j \\ \frac{(1-p)}{3} & \text{if } i \neq j, \end{cases}$$



where $Pr[j_R|i_S]$ is the conditional probability that the number j is received given that the number i is sent. The figure on the right indicates that source numbers are either transmitted correctly (horizontal lines) with probability p or corrupted (diagonal lines) with probability $(1-p)/3$ for each other number.

1. Determine $Pr[0_R]$, the probability the receiver receives a 0 for any randomly-selected tick of the clock.

2. Determine $Pr[\varepsilon]$, the probability of an error occuring on any randomly-selected tick of the clock.

3. Determine a reasonably simple expression for $Pr[A_n]$, where A_n denotes the event that there is at least one error in a sequence of n transmissions at n ticks of the clock.

4. Determine a reasonably simple expression for $Pr[i_S|j_R]$ where $i \neq j$ (in the box).

11. Probability: nihilism, almost. 17 points: 3/3/4/4/3

While eating chicken nuggets at McDonald's, Jonathan challenges Emaan to a game.

Jonathan has a standard 52-card deck, with 26 red cards and 26 black cards. He shuffles the deck and will flip cards one at a time from the top.

Emaan's goal is to call when Jonathan is going to flip over a red card. Before each flip, Emaan can either "pass", meaning Jonathan flips over the next card for Emaan to see, or "bet", meaning Jonathan shows Emaan the next card and if it is red, Emaan wins, and if it is black, he loses. If Emaan never calls "bet", then he loses.

Emaan starts thinking of some strategies, like, he's going to wait until he sees 5 more black cards than red cards, and then once he does, he will call "bet".

1. Let's say Emaan has seen 15 black cards and 10 red cards. If he calls bet, what is the chance he wins the game?

2. Let's say Emaan has seen b black cards and r red cards so far, and there are still cards remaining. What is the probability that the next card in the deck is red?

3. Use the previous part to show that no matter what strategy Emaan employs, his chance of winning is always $\frac{1}{2}$.

4. Now let's change the game. Now Emaan's goal is to get the next card to be the same color as the previous card. So, when he calls "bet", he wins if the next card Jonathan shows is the same color as the previous card shown. Therefore, Emaan cannot "bet" on the first turn, he must "pass", since there is no previous card. Prove that Emaan might as well wait until the last two cards before betting. (Note that here Emaan will either bet when two cards are left or when one card is left.)

5. Given Emaan plays optimally, find the probability Emaan wins.