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

PRINT Your Name: Oski Bear

SIGN Your Name: *OSKI*

PRINT Your Student ID: _____

CIRCLE your exam room:
Pimentel 1 GPB 100 Hearst Annex A1 Soda 320 Latimer 120 Other

Name of the person sitting to your left: Papa Bear

Name of the person sitting to your right: Mama Bear

- 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.
- On questions 1-2: You need only give the answer in the format requested (e.g., true/false, an expression, a statement.) We note that an expression may simply be a number or an expression with a relevant variable in it. **For short answer questions, correct clearly identified answers will receive full credit with no justification. Incorrect answers may receive partial credit.**
- On question 3-8, do give arguments, proofs or clear descriptions as requested.
- You may consult one sheet of notes. Apart from that, you may not look at books, notes, etc. Calculators, phones, and computers are not permitted.
- There are **14** 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 8 questions on this exam worth a total of 115 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.
   Answer: True. 7 has a multiplicative inverse mod 10 since $gcd(7,10) = 1$.
2. The function $f(x) = ax \pmod{N}$ is always a bijection if $gcd(a,N) = 1$.
   Answer: True. a has a multiplicative inverse modulo N.
3. If there are k numbers that are relatively prime to N in $\{0,\ldots,N-1\}$, then $a^k = 1 \pmod{N}$ if $gcd(a,N) = 1$.
   Answer: True. The proof of Fermat's theorem works since $ax \pmod{N}$ is a bijection on the relatively prime elements and each has a multiplicative inverse.
4. For all $n > 2$, there is at least one element of $\{2,3,\ldots,n-1\}$ with a multiplicative inverse $\pmod{n}$.
   Answer: True. $gcd(n,n-1) = 1$ which means $n-1$ has a multiplicative inverse. Indeed, the inverse is $n-1$ since $n-1$ is congruent to $-1 \pmod{n}$.
5. It is possible to measure out exactly 1 oz. of water using only cups of size 56 oz. and 14 oz.
   Answer: False. $\gcd(56,14) = 7 \neq 1$. Effectively, we are asking if $\exists x,y \in \mathbb{Z}$ where $56x + 14y = 1$. We know this can only be true if the gcd is 1.
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.
   Answer: False. $x^3 + 1 \pmod{5}$ has one root.
7. If two degree d polynomials intersect on $d+1$ points, they must be the same polynomial.
   Answer: True. For two polynomials, $P(x)$ and $Q(x)$, we have $P(x) - Q(x)$ has $d+1$ roots and has degree d and thus must be the zero polynomial.
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.
   Answer: False. One can just run the program for k^k steps an an interpreter.
9. For any countable subset, S, of the reals, $\mathbb{R}$, we have $\exists \varepsilon > 0 \in \mathbb{R}, \forall x,y \in S, (x \neq y) \implies (|x-y| \geq \varepsilon)$.
   Answer: False. The rationals are a subset of the reals and countable.

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.

    Answer: True. There are a countable number of inputs.

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

    Answer: False. The inequality is the reverse of what is true. Any sample point in the set $(A \cap B) \cup C$ is contained in $A \cup C$.

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

    Answer: True. We know $\bar{A}$ is also independent of B and C and any two disjoint intersections of mutually independent events are independent from the definition of mutually independent events.

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

    Answer: False. Take $A = B$ as an example where $P[A] < 1$.

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

    Answer: True. Note that the probability of A is the weighted average of $Pr[A|B]$ and $Pr[A|\bar{B}]$, i.e., $Pr[A] = Pr[A|B]Pr[B] + Pr[A|\bar{B}](1 - Pr[B])$. If one term is higher than average than the other must be lower. One could also do algebra here.

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 $\gcd(0,n)$?
   Answer: $n \mid 0 \iff \exists k \in \mathbb{Z}, kn = 0$. Regardless of what n is, $k = 0$ works so $n \mid 0$ always. Therefore $\gcd(0,n) = n - 0$ is never coprime with $n > 1$.
2. What are the possible values of $\gcd(n, n+2)$?
   Answer: $\{1,2\}$. $\gcd(n,n+2) = \gcd(2,n) \in \{1,2\}$
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.**
   Answer: $ka \pmod{y}$. Since $kax + kby = kd = (ka)x \pmod{y}$, thus $z = ka \pmod{y}$ works.
4. What is the smallest possible positive value of the expression $14x \pmod{21}$ in $\{1,\ldots,20\}$?
   Answer: 7. The smallest value is $gcd(14,21)$, since there is $a(14) + b(21) = 2$ according to the extended gcd theorem.
5. What is $7^{11} \pmod{15}$?
   Answer: 13. When $a \neq 0$, $a^{(p-1)(q-1)} = 1 \pmod{pq}$, or $7^8 = 1 \pmod{15}$ and $7^3 = (49)7 = (4)(7) = 13 \pmod{15}$
6. Find $x \pmod{90}$ where $x = 1 \pmod{9}$ and $x = 3 \pmod{10}$.
   Answer: 73. 4, and $10^{-1} = 1 \pmod{9}$ and $9^{-1} = 9 \pmod{10}$ and $u = 1(10)(1) + 3(9)(9) = -17 = 73 \pmod{90}$.

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

   Answer: 24. The number of relatively prime numbers in the range $\{0,\ldots,pq-1\}$ is $(p-1)(q-1)$. This is $(5-1)(7-1)=24$.

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

   Answer: 9. Take the expression $9999^9 = 99^9 = -1^9 = -1 = 99 \pmod{100}$.

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

   Answer: $p-1$. By FLT, we know the polynomial $x^{p-1}-1 \pmod{p}$ has roots at all x coprime with p.

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?

    Answer: $x^{p-1}-1 \pmod{p}$.

    By FLT, we know the polynomial $x^{p-1}-1 \pmod{p}$ has roots at all x coprime with p. Since both this and the polynomial in question are degree $p-1$, have a leading coefficient of 1, and they share $p-1$ roots, they must be the same. So the result must be $x^{p-1}-1 \pmod{p}$.

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?

    Answer: $n+p+2q$. We can immediately detect where the erasure errors are, and are left with $n+2q$ symbols that we can apply Berlekamp Welch on to figure out the polynomial.

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.)
    Answer: $2n$.

    (b) Consider $y = a \pmod p$, we know that $y^d = a^d \pmod p$. Prove that $y^d = a^u \pmod p$ where $u = d \pmod{p-1}$.
    Answer: If $y = 0$, this is clearly true. Otherwise $y^d = a^d = a^{u+k(p-1)} = a^u(a^{p-1})^k = a^u(1)^k = a^u \pmod p$.
    The second to last equality is from Fermat's Little Theorem. The rest is algebra.

    (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 $v = d \pmod{q-1}$.
    Answer: $m_1 q(q^{-1} \pmod p) + m_2(p)(p^{-1}) \pmod q) \pmod{pq}$. This is from the CRT theorem.

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?

    Answer: Eve listens for people's credit cards and gets one or more people's credit cards albeit in the form $x^e \pmod N$, then she can buy as many books as she wants from Alice by presenting $x^e \pmod N$ from one of the people. When Alice decodes she gets someones valid credit card and charges them.

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.) **Answer:** $r = d_1 + d_2 + 1$ and $q = d_2 + 1$.
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 $P(3) = 4 \pmod 5$?
   Answer: 0. This is the line $P(x) = 3x \pmod 5$
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?
   Answer: $p \geq \max(2^b, n+k)$. each packet should be able to encode a b bit number and one needs to be able to send $n+k$ packets.
4. What is the maximum number of points at which two distinct degree d polynomials can intersect?
   Answer: d times. Otherwise $P(x) - Q(x)$ would have more than d roots.
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 $x = 2$.)
   Answer: $(p-1)\binom{p+d-1}{p-1}$. We have to choose d roots with repetition from p possibilities. The number is $\binom{p+d-1}{p-1}$. Then we can scale by any of $p-1$ values.

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=".)

   Answer: $\frac{15!}{2!2!2!}$

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?

   Answer: $n!(n-1)!$. At the i-th turn there are $n-i+1$ options for person who got eliminated and $n-i$ options for the person who won.

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

   Answer: 280. Order the 9 people (9! ways to do this). Take the first three to be the first team, second three to be the second team, and third three to be the third team. But we overcounted. Each team of three can order its three people in 3! ways and the three teams can be swapped around in 3! ways, so we divide 9! by $(3!)^4$, which gives us $9!/(3!^4) = 280$.

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 $\pmod 3$?
   Answer: $4(3)(3) = 36$ ways.

   (b) Case 2: How many 3-element subsets of S have all the elements being equivalent $\pmod 3$?
   Answer: 6. $\binom{4}{3} = 4$ ways if elements are 0 $\pmod 3$ and $\binom{3}{3} = 1$ way otherwise (total of 6).

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?
   Answer:
   If every vertex has degree 1, then this means we get three pairs of vertices. There are $\binom{6}{2} = 15$ ways to pick the first two to be together, then $\binom{4}{2} = 6$ ways to pick the next two, and the last two are determined. This gives us $6 \cdot 15 = 90$, but we overcounted by a factor of 6 because the order in which we picked the pairs doesn't matter. So 15 for this case.

   (b) How many ways can we form two disjoint cycles of length three with six vertices?
   Answer: 10. There are $\binom{6}{3} = 20$ ways to pick two groups, but we overcounted by 2, since picking one group of 3 is equivalent to picking the ones not picked. So, $20/2 = 10$ counts for this one. Note there is only one possible cycle for each group, K_3.

   (c) How many ways can we form a long cycle of length six?
   Answer: $60 = \frac{6!}{2\times 6}$. We think of the cycle as a permutation of the vertices, which has 6! possibilities. However, where you start in the permutation doesn't matter, so divide by 6. Then, the direction in which you travel along the cycle also doesn't matter, so divide by 2.

   (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.)
   Answer: 172. Here we count the graphs of degree up to 3 and notice that the graphs of degree more than 3 can be counted using the edges that are left out, and thus we double the result. The graphs of degree up to 3 include a,b,c and the graph of degree 0. This sums to 86. Multiply by 2 to yield result.

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.
   Answer: $\binom{n}{k} = \binom{n}{n-k}$.
2. Use a combinatorial argument to prove that $\binom{n+m}{k} = \sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i}$
   Answer: The LHS is choosing k elements from $n+m$, the right hand side does the same by enumerating over the values for i where i are chosen from the first n and j are chosen from the last m.
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.)
   Answer: $n2^{n-1}$. The left hand side counts the number of ways to choose a k sized subset of n elements and two elements from that set with possible repetition. The first term counts the same without repetition. X counts the number of subsets with repetition.

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 $Pr[A \cap B]$?
   Answer: 1/6. $Pr[A \cap B] = Pr[A|B]Pr[B]$.
2. Given $Pr[A|B] = 1/3$, $Pr[B] = 1/2$ and $Pr[A|\bar{B}] = 1/2$, what is $Pr[B|A]$?
   Answer: 2/5. $Pr[A] = Pr[A \cap B] + Pr[A \cap \bar{B}] = 1/6 + 1/4 = 5/12$. $Pr[B|A] = Pr[A \cap B]/Pr[A] = \frac{1/6}{5/12} = 2/5$.
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.
   Answer: 1/6. The number of elements is 100. For each permutation, there are 1 out of 6 ways to for 1, 2 and 3 to be in order.
4. What is the size of the sample space for rolling four distinguishable dice?
   Answer: 6^4
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?
   Answer: $(5/6)^3(1/6)^1$. You compute the probability that the first three are not six and that the fourth is six.
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?
   Answer: $\binom{3}{1}(5/6)^2(1/6)^2$. You have to have a six in the first four and a six in the last position. There are $\binom{3}{1}$ such sample points and each has probability $(5/6)^2(1/2)^6$.
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"?
   Answer: 91/216. Consider the complement. If no two consecutive rolls have the same number, this means each roll after the first must be one of five numbers. So the probability a sequence of 4 dice rolls is not lucky is $1 \cdot (5/6)^3 = 125/216$, and the probability that it is lucky is $1 - 125/216 = 91/216$.
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?
   Answer: 1/4. The experiments outcomes can be described by die and side which are all equally likely and yield a sample space of size 24. 6 of them have six on them. Dividing yields 1/4.
   (b) You get a six on the first roll. What is the conditional probability that you chose a cheating die?
   Answer: $\frac{2}{3}$. As before, the experiment's outcome can be described by die, side. Each outcome is equally likely. Event A is that the side you see is six. The event B is that the other side is six. We are asked $Pr[B|A] = Pr[A \cap B]/Pr[A] = (4/24)/(1/4) = 2/3$.
   (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).**
   Answer: 5/18.
   Let B be the event it is a two-sided die and A be the event we see a six. Oh. Yeah. We just calculated $Pr[B|A]$ to be $1/3$.
   The total probability of a six(let's call the event H) with another flip is $Pr[B]Pr[H|B] + Pr[B^c]Pr[H|B^c] = (2/3) \times (1/3) + (1/3)(1/6) = 5/18$.

(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).**
Answer: $\frac{4}{5}$.
We can update from the previous. Again, the event B corresponds to this being a double sided die, where the $Pr[B] = 2/3$ prior to this roll. We let A be the event that we see a six on the second roll. Also $Pr[A|B] = 1/3$.
And, $Pr[B|A] = Pr[A|B]Pr[B]/Pr[A]$, where $Pr[A] = 5/18$ from the previous part $Pr[B] = 2/3$ from the previous previous part. We get $(2/9)/(5/18)$ which is $4/5$.
Also acceptable is $(1/3)(b)/(c)$.

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?
Answer: $\frac{1}{n}$.

(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.)
Answer: $\frac{k}{n}$.